

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

FILED BY SM D.C.

Oct 21, 2026

ANGELA E. NOBLE
CLERK U.S. DIST. CT.
S. D. OF FLA. - FTL

UNITED STATES OF AMERICA

v.

PAVEL ALEKSEYEVICH KULIZHNIKOV,
a/k/a "Pavel Alekseevich
Kulizhnikov,"
a/k/a "Pasha,"
a/k/a "Panprezident1,"

[REDACTED],
a/k/a [REDACTED],
a/k/a [REDACTED],
a/k/a [REDACTED]

and

[REDACTED],
a/k/a [REDACTED],
a/k/a [REDACTED],
a/k/a [REDACTED]

Defendants.

Case No. 1:26-MJ-407

FLSD Case Number: 26-mj-6603-Augustin-Birch
UNDER SEAL

ORDER TO SEAL

The UNITED STATES, pursuant to Local Rule 49(B) of the Local Criminal Rules for the United States District Court for the Eastern District of Virginia, having moved to seal the Complaint, Affidavit in Support of the Complaint, arrest warrants, the Motion to Seal, and proposed Order in this matter; and

The COURT, having found that revealing the material sought to be sealed would jeopardize an ongoing criminal investigation; having considered the available alternatives that are less drastic than sealing, and finding none would suffice to protect the government's legitimate interest in concluding the investigation; and finding that this legitimate government interest outweighs at this

time any interest in the disclosure of the material; it is hereby

ORDERED that the Complaint, Affidavit in Support of the Complaint, arrest warrants, Motion to Seal, and this Order be sealed until the defendants are brought to the Eastern District of Virginia.

John Anderson

Digitally signed by John
Anderson
Date: 2026.10.14 11:49:43
-04'00'

John F. Anderson
United States Magistrate Judge

Date: October 14, 2026
Alexandria, Virginia

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

United States of America

v.

PAVEL ALEKSEYEVICH KULIZHNIKOV, a/k/a "Pavel Alekseevich
Kulizhnikov," a/k/a "Pasha," a/k/a "Panprezident1,"

and

Defendant(s)

Case No. 1:26-mj-407

UNDER SEAL

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 05/24-present / 6/13/24 & 7/16/24 in the city/county of Alexandria & Fairfax County

in the Eastern District of Virginia, the defendant(s) violated:

Code Section

Offense Description

Defendants KULIZHNIKOV and [REDACTED]: Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h), with two objects: concealment, in violation of 18 U.S.C. § 1956(a)(1)(B)(i), and sting, in violation of 18 U.S.C. § (a)(3)(B).

Defendant [REDACTED]: Conspiracy to Conduct an Unlicensed Money Transmitting Business, in violation of 18 U.S.C. §§ 371, 1960.

This criminal complaint is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.

Reviewed by AUSA/SAUSA

AUSA Edgardo J. Rodriguez

Printed name and title

Melissa Schneider

Complainant's signature

DEA Special Agent Melissa Schneider

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

telephone (specify reliable electronic means).

Date: 10/14/2026

John Anderson

Digitally signed by John
Anderson

Date: 2026.10.14 11:46:59 -04'00'

Judge's signature

City and state: Alexandria, Virginia

The Hon. John F. Anderson, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

Case No. 1:26-MJ-407

PAVEL ALEKSEYEVICH KULIZHNIKOV,
a/k/a “Pavel Alekseevich Kulizhnikov,”
a/k/a “Pasha,”
a/k/a “Panprezident1,”

UNDER SEAL

[REDACTED]
a/k/a “[REDACTED],”
a/k/a “[REDACTED],”
a/k/a “[REDACTED],”

and

[REDACTED]
a/k/a “[REDACTED],”
a/k/a “[REDACTED],”
a/k/a “[REDACTED],”

Defendants.

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND ARREST WARRANTS

I, Melissa Schneider, a Special Agent with the United States Drug Enforcement Administration (“DEA”), being first duly sworn, hereby depose and state the following:

INTRODUCTION

1. This affidavit is submitted in support of a criminal complaint and arrest warrants for **Pavel Alekseyevich KULIZHNIKOV a/k/a “Pavel Alekseevich Kulizhnikov” a/k/a/ “Pasha” a/k/a “Panprezident1” (“KULIZHNIKOV”);** [REDACTED]

[REDACTED] and [REDACTED]
[REDACTED]

2. Based on the information set forth in this affidavit, I submit there is probable cause to believe that, beginning on a date unknown but from at least in or around May 2024 and continuing thereafter up to and including the present, in the Eastern District of Virginia and elsewhere, **KULIZHNIKOV** and [REDACTED] knowingly and intentionally combined, conspired, confederated, and agreed with each other and others, both known and unknown, to commit an offense against the United States in violation of 18 U.S.C. § 1956(h), to wit:

- a. to conduct financial transactions affecting interstate or foreign commerce, which involves the proceeds of specified unlawful activity, that is, the distribution of controlled substances and conspiracy to do the same, knowing that the transactions were designed in whole or in part to conceal or disguise the nature, location, source, ownership, or control of the proceeds of specified unlawful activity, and knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of 18 U.S.C. § 1956(a)(1)(B)(i); and
- b. to conduct financial transactions affecting interstate or foreign commerce, which involved property represented to be proceeds of specified unlawful activity, that is, the distribution of controlled substances and conspiracy to do the same, with intent to conceal or disguise the nature, location, source, ownership, or control of property believed to be the proceeds of specified unlawful activity, in violation of 18 U.S.C. § 1956(a)(3)(B).

3. I further submit that there is probable cause to believe that on or about June 13, 2024, and on or about July 16, 2024, that [REDACTED] unlawfully, knowingly, and intentionally combined, conspired, confederated, and agreed with others, known and unknown, within the Eastern District of Virginia and elsewhere, to commit violations of 18 U.S.C. §§ 371 and 1960 (Conspiracy to Conduct an Unlicensed Money Transmitting Business).

AGENT BACKGROUND

4. I am a Special Agent with the Drug Enforcement Administration (“DEA”) and have been since July 2004. During my employment with DEA, I have received several hundred hours of comprehensive, formal instruction on such topics as drug identification, patterns of drug trafficking, money laundering techniques, cryptocurrencies and blockchain analysis, complex conspiracies, the exploitation of narcotics traffickers’ telecommunications devices, criminal law, surveillance, and other investigative techniques. I have initiated and assisted in numerous investigations into the unlawful importation, manufacture, possession with intent to distribute, and distribution of narcotics (including cocaine, heroin, opium, marijuana, and methamphetamine), the laundering of narcotics proceeds, and conspiracies associated with narcotics offenses, and I have served as the affiant for numerous federal Title III and California state wiretap orders and search warrants. In conducting these investigations, I have utilized a variety of investigative techniques and resources, including but not limited to such techniques as surveillance, confidential sources, search warrants, telephone toll analysis, and wire intercept communications analysis in Title III and California state wiretap investigations.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested arrest warrants and criminal complaint and does not set forth all of my knowledge about this matter. The facts set forth below are based upon (1) my own personal observations; (2)

reports and information provided to me by other law enforcement agents or government agencies; (3) other documents obtained during the course of the investigation; (4) confidential source (CS) debriefings; and (5) consensually recorded audio, video, and electronic communications.¹

PROBABLE CAUSE

Background of the Investigation

6. DEA is currently conducting a joint investigation with the U.S. Customs and Border Protection (“CBP”), Internal Revenue Service – Criminal Investigation (“IRS-CI”), and Federal Bureau of Investigation (“FBI”) into a Russian money laundering organization (the “MLO”) involved in the laundering of proceeds from drug trafficking and other illicit activity in and through the U.S. (including the Eastern District of Virginia), the Russian Federation, the Republic of Colombia, the United Kingdom, various other European countries, the United Arab Emirates, the Commonwealth of Australia, and elsewhere via bulk cash remittances and cryptocurrency²

¹ References to monitored conversations are based on conversations with and preliminary transcripts made by DEA agents, Task Force Officers (“TFOs”), and contracted personnel. Subsequent review of the recorded conversations and the preparation of verbatim transcripts may well lead to minor changes. Where recorded conversations are cited, I have included my interpretation (based on my training, experience, and knowledge of this case) in brackets and following the excerpts. All figures, times, and calculations set forth herein are approximate.

² Cryptocurrency (also known as digital or virtual currency) is an electronic-sourced unit of value that can be used as a substitute for fiat currency (i.e. currency created and regulated by a government) to buy goods or services or exchanged for fiat currency or other cryptocurrencies. Bitcoin (BTC) and Tether (USDT) are types of cryptocurrencies. Cryptocurrency is generated and controlled through computer software operating on a decentralized peer-to-peer network. Most payments are recorded on a distributed public ledger online (“blockchain”) that is maintained by peer-to-peer verification, and thus not maintained by a single administrator or from a single location. Cryptocurrency only exists digitally (rather than in physical form), is transacted and stored on blockchains, and is sent/received through a virtual “wallet”. A cryptocurrency wallet is a device or service that essentially stores the access code allowing an individual to interact with blockchains and conduct cryptocurrency transactions. The wallet generates and/or stores a “public key” (akin to a bank account number) and a “private key” (akin to the password accessing that account). The wallet can be housed on an external electronic storage device (“hardware wallet”), downloaded on a PC or laptop (“desktop wallet”), with an Internet-based cloud storage provider, or in an online account associated with an Internet-based cryptocurrency exchange (e.g. Binance, Coinbase, Bybit). Transactions can be conducted on any type of computer, including laptop computers and smart phones. Cryptocurrency is not illegal in the United States and may be used for legitimate financial transactions. However, since cryptocurrency is decentralized and virtual (and thus can be accessed from any location), it is often used

transactions. As detailed herein, the investigation has revealed the MLO is comprised of several “teams,” some of which are structured further into subgroups with various managers and couriers (“cashiers”) for bulk currency transfers. Individual members sometimes maintain their own clients and focus on one or more particular cities in which they personally conduct bulk currency transfers and/or direct subordinate cashiers/couriers—but they regularly coordinate with other MLO managers/teams to fulfill contracts in cities outside their own established markets, commonly following established MLO procedures for making the client referrals and conducting transactions (e.g., creating a Telegram³ group chat to facilitate the logistics of the transfer). This understanding between members—and access to a collective, international cashier/courier network—exponentially increases members’ profits and has established the MLO as a global enterprise capable of laundering billions of dollars.

7. The investigation has also led to the identification of the following MLO members and their roles:

- a. Unidentified Co-Conspirator 1 (UCC-1) is a leader of an MLO team known as the JUST WORLD PRO CRYPTO TEAM or JUST HOLLYWOOD STARS (the “JUST Team”). The JUST Team operates around the world but specializes in laundering illicit proceeds (including drug proceeds) in the United States, Colombia, Spain, and the United Arab Emirates. UCC-1 personally facilitates

for conducting illegal transactions (including the sale of controlled substances).

³ WhatsApp and Telegram are encrypted, Internet-based, data applications that enable iPhone, Android, and Windows Mobile users to exchange electronic messages and voice calls. Each Telegram account has a username (or “handle”), which is a unique identifier at least five characters long. The username/handle begins with the @ symbol. Alternatively, users can send contacts a direct link (formatted as *t.me/username* or *username.t.me*); clicking on this direct link automatically opens the Telegram application and starts a chat with that user. Users may also select a screen name (or display name) for their account. The screen name appears in their chat threads, but is not unique to the user, and can be changed at any time by the owner.

introductions between various regional managers and cashiers/couriers of the JUST Team, among other responsibilities. UCC-1 also coordinates transactions with other MLO members and teams.

- b. **KULIZHNIKOV** is a cryptocurrency reseller/broker affiliated with the JUST Team, primarily based in the Miami, Florida, area but operating throughout the United States. **KULIZHNIKOV** dispatches cashiers/couriers to conduct bulk cash transfers to/from clients, personally conducts some of those bulk cash transfers himself, and coordinates bank wire or cryptocurrency payouts through his own or his partners' accounts.
- c. [REDACTED] is one of **KULIZHNIKOV**'s brokers in the Miami area, responsible for negotiating transactions with money laundering clients and coordinating cashiers/couriers involved in bulk currency transfers with clients.
- d. [REDACTED] is a cashier/courier in the Miami area affiliated with **KULIZHNIKOV**, responsible for picking up and/or delivering bulk cash to clients and/or other MLO members.

Identification of the MLO

8. From January 2021 to September 2022, DEA coordinated a series of five (5) reverse undercover money laundering operations (totaling approximately \$900,000), wherein one or more brokers affiliated with the MLO coordinated the pickup of bulk currency (purported to be drug proceeds, but actually constituting government funds) from cities across the United States and remitted payouts in cryptocurrency or cash delivered in other cities. The first transaction in this series involved the April 2021 delivery of approximately \$170,000 by a DEA undercover officer to a courier in the Los Angeles, California, area, to be remitted in the Miami area.

9. On or about May 5, 2021, after another MLO broker informed an undercover officer in Miami that he would send a cashier/courier to complete the payout for this first transaction, the undercover officer was contacted via WhatsApp by another co-conspirator (“UCC-2”). The undercover officer was also contacted by UCC-1 (using a WhatsApp account). During a series of WhatsApp texts and consensually recorded calls, UCC-1 confirmed that UCC-2 was UCC-1’s worker, the “papers” [cash] were ready, and the amount was approximately \$164,900 (i.e., the transaction payout after deducting a 3% commission). On or about May 6, 2021, UCC-2 delivered approximately \$164,900 to the undercover officer in Hallandale Beach, Florida.

10. Immediately after the pickup, the undercover placed a consensually recorded WhatsApp call to UCC-1 to thank UCC-1 for coordinating the transaction and discuss conducting additional cryptocurrency transactions. UCC-1 stated, “Not too much person work seriously, you know? Mostly these guys [other brokers] are temporary – and we work for years. We do cash-cash, and then we found the crypto, and do now with the crypto.” The undercover officer replied, “Yes, right now the crypto’s taking over. But you know, you have to find the right person, because there has to be a lot of trust.” UCC-1 stated, “I am the most famous in crypto guy – you can ask.” UCC-1 noted UCC-1 was currently in Moscow, Russia, but “I have a representative - my cashier” in Miami. UCC-1 further explained, “Not the guy [UCC-2] who bring today the money, no. More representative, he now is in Hallandale [Florida]. You can meet with him – we can build a trust.”

11. On or about May 10, 2021, UCC-1 called the undercover officer. During the consensually recorded call, UCC-1 continued explaining the MLO’s operating structure. UCC-1 stated, “We have two offices in Moscow, one in Belarus, one in Barcelona, one in London. We have a lot of – also in Miami, we have a cashier, it’s my friend. I want him to represent us in the meeting.” The undercover officer replied, “So I can sit down with him [referring to UCC-1’s

Miami-based representative], and whatever goes, it's the same thing with you, correct? The same terms and everything?" UCC-1 confirmed, "Yes, correct, correct, yes All same responsibility. One hundred percent trust." The undercover officer replied, "Perfect. Let's do this." UCC-1 suggested, "If you tell me or write me a plan – I mean, which destination you need, which destination do you have, what currency – I will prepare for you already information, prices, and our possibilities We work 40 countries, we work."

12. Later in the call, UCC-1 asked the undercover officer, "You always need cash in Miami – not have, yes?" The undercover officer replied, "Depends. Sometimes I have to – I have cash in Miami, and I have to pay out in Colombia. Or I have cash in Europe, and I have to pay out in Colombia or Central America." UCC-1 offered, "We feel very comfortable in Bogota, Cali, Cucuta, and Medellin. Barranquilla, too. We can accept any transfer to there from wherever you want – United States, Europe. In Europe we have – no, ok. This information I will write, or my – [UCC-2] will give you. I already feel that we have a connection."

13. Beginning in or around 2025, a DEA confidential source ("CS7")⁴ identified UCC-1 as a money launderer who has been a member of the MLO since at least early 2020. CS7 explained that the MLO operates on a private Telegram group chat and is comprised of several teams providing international cryptocurrency/cash exchange services. CS7 estimated that each

⁴ The "CS" numbers in this affidavit correspond to a particular DEA number assigned to each CS in this investigation and are not numbered in sequence of appearance in this document. CS7 is working in hopes of earning sentencing consideration in his/her own case, which involves money laundering charges and sanctions pursuant to Executive Order 14024 (for operating or having operated in the financial services sector of the Russian Federation economy by conducting international money laundering transactions and providing material support to another OFAC-designated individual). CS7 has provided agents (including me) with extensive intelligence regarding the Target Subjects. The statements made by CS7 have been internally consistent, and consistent with statements made throughout different debriefings. CS7's statements also contain extensive detail that I believe could only be obtained through first-hand knowledge and involvement with the Target Subjects and substantial portions of which agents have been able to corroborate through other means (e.g., electronic communications with MLO members). In sum, I believe CS7 to be reliable.

team conducts approximately ten (10) to fifty (50) transactions per day. CS7 explained that if an affiliated money launderer receives a bulk currency request that he or she is unable to process, the contract would be advertised on the MLO's Telegram group chat, and another team with an available cashier/courier in that location would accept and coordinate the cash pickup from the client. A separate, limited group chat (i.e., between the initial MLO member brokering the transaction, the client, and the executing MLO member) would be created to facilitate the transaction logistics.

14. CS7 advised that if any payment disputes arise, a panel of approximately ten (10) to fifteen (15) MLO members is formed to mediate and issue a ruling. Usually, MLO members accept these ad hoc panels' rulings, and the parties deemed at fault pay the settlement, since it is more profitable to accept a fine and remain part of the MLO than to leave and operate independently. However, if the disputes are not resolved through internal mediation, then the member deemed at fault is expelled from the organization. For example, CS7 described a transaction in or about 2021, in which UCC-1 coordinated the laundering of approximately \$700,000 from Moscow to London through the MLO via multiple installments. UCC-1 coordinated the payout with one of the MLO's original founders, who stole the final \$200,000 installment. CS7 noted that this founding member ultimately stole a total of \$50 million from the MLO and, accordingly, was removed from the Telegram group and expelled from the MLO.

15. CS7 identified UCC-1 as the leader of the JUST Team within the MLO. CS7 further advised that the JUST Team is the biggest within the MLO for bulk currency transactions outside of Russia, operating in the United States, the United Kingdom, throughout Europe, Colombia, Ecuador, and Latin America. The JUST Team is comprised of approximately ten (10) principals, but they have cashiers/couriers in each country to pick up bulk cash. CS7 noted that although some

MLO members are wary of operating in Latin America, since too many of the clients there are involved with drugs and guns and therefore are more likely to draw law enforcement attention, UCC-1 readily accepted these contracts. CS7 estimated the JUST Team launders approximately \$50 million per day.

16. CS7 advised that UCC-1 has no other business besides the JUST Team, and UCC-1 has many partners on the team. UCC-1 and the JUST Team have intentionally developed their branding, so that clients and cashiers/couriers will easily recognize someone messaging them (i.e., with instructions regarding where to deliver cash) as a member of the JUST Team. For example, members often include the Team name (e.g., “Just”) in their Telegram usernames/handles.

17. CS7 identified UCC-1’s username. As recently as in or around July 2026, I observed that the publicly viewable contact details of UCC-1’s Telegram account included “Just world pro crypto team” in the biography section. The biography sections of other identified JUST Team members’ Telegram accounts similarly state “Just world pro crypto team.” Several members have also adopted Telegram screennames and profile pictures based on movie stars (e.g., Al Pacino), and members also frequently incorporate their roles (e.g., cashier, manager) into their Telegram username. For example, one of **KULIZHNIKOV’s** Telegram usernames is @TheAlienEx_manager; as recently as in or around July 2026, I observed that his publicly viewable Telegram biography advertises “EXCHANGE USDT [U.S. flag emoji] MIAMI” and even lists “business hours” (e.g., 10:00 a.m. to 8:00 p.m. Monday through Friday). CS7 further advised that other MLO teams similarly employ this sort of branding (e.g., incorporating the team name into their Telegram usernames, using a team logo as their Telegram profile photos, identifying “cashier” or other roles in Telegram usernames).

18. CS7 described numerous money laundering transactions, involving multi-million-dollar sums of bulk currency, conducted with and through the MLO (including UCC-1) during the period 2020-2023. CS7 also provided electronic communications and records pertaining to some of these transactions. For example, consensually downloaded Telegram chats with UCC-1 revealed that UCC-1 also helped facilitate the fourth reverse undercover money laundering transaction conducted by DEA, which was initiated in or around November 2021 in the Los Angeles area. Specifically, UCC-1 forwarded the phone number ([REDACTED]) of an MLO cashier to the MLO broker coordinating the undercover transaction. An undercover officer contacted the cashier at the x [REDACTED] phone number provided by UCC-1 and arranged a meeting on or about December 2, 2021, to deliver approximately \$190,000 (purported to be funds for the transportation of a drug shipment). The funds were subsequently remitted by the MLO partially via BTC (Bitcoin) and USDT (Tether) cryptocurrency transfers to an undercover cryptocurrency wallet and partially in cash delivered to another undercover officer in Madrid, Spain.

19. The consensually downloaded Telegram chats with UCC-1 also referenced logistical details for numerous other international money laundering transactions in locations such as Miami, London, Colombia, the Dominican Republic, and Ecuador. For example, a message forwarded to UCC-1 in or around November 2021 requested, "Send a photo of the token for this 1 billion transfer." Based on my training and experience, I know that sophisticated money launderers typically provide the serial number from a banknote (known as a "token") to clients when discussing the logistics involved in the pickup of bulk cash. The token serves as a code for the broker's and client's couriers conducting the physical transfer, as well as a receipt for the client's courier to prove that he delivered the cash as instructed to the correct recipient. Tokens were also exchanged in the undercover transactions conducted in this investigation.

20. The Telegram chats with UCC-1 also included forwarded messages detailing contract registrations, formatted with a transaction number and designation indicating whether the client would be delivering (“in”) or receiving (“out”) bulk cash. For example, UCC-1 forwarded a message in or around November 2021 that included an invitation link to a Telegram group chat, with the following details:

#Order CSH-21905-OUT

Location: ES:Barcelona(V) | EUR

Amount: 200000

Contact: [UCC-1]

21. In or before November 2025, an unknown subject created a publicly viewable website entitled, “Just Hollywood Stars Database Leak” and posted a ledger documenting approximately 12,165 transactions dated from approximately April 2024 to August 2025. The listed transactions are identified by the same contract registration format as some of the transactions in UCC-1’s Telegram messages. Namely, the transactions are numbered and designated according to whether the client would deliver (“in”) cash to the MLO (to be remitted in cryptocurrency) or receive a cash remittance (“out”) from the MLO (as payment for a cryptocurrency transfer), such as “CSH-72185-OUT.” The ledger lists transaction dates, cashier/location, coded names for “manager” and “client,” transaction sum, currency (including but not limited to U.S. dollars, British pounds, Euros, and Russian rubles). The total sum of the U.S. dollar transactions alone is approximately \$148,683,415.

- a. The ledger lists UCC-1 as the manager for approximately 1,246 cash transactions in numerous countries and currencies, including forty-one (41) U.S. dollar transactions totaling approximately \$3,509,834 from approximately

April 2024 to July 2025. The cashier/location for three of those transactions (totaling approximately \$463,000) is identified as “US:Miami.”

- b. The ledger also lists numerous transactions for other identified MLO members/teams and/or clients assigned code names referencing the MLO. The transaction details indicate they were coordinated by multiple managers and assigned cashiers from Miami, Houston, and several foreign cities.

Identification of KULIZHNIKOV as an Affiliate of the MLO's JUST Team

22. Beginning in or around 2025, CS11⁵ described how “cashiers” (i.e., couriers) are recruited to work for the JUST Team in multiple cities in the United States. CS11 explained that transactions are coordinated by JUST Team managers located outside the United States and in amounts ranging from approximately \$20,000 to \$200,000 per transaction. The cashiers receive instructions from managers to deliver bulk currency to particular buyers/brokers. CS11 also described an internal dispute on the JUST Team with two particular managers, who were subsequently expelled from the MLO in or about late 2025 (i.e., contemporaneously with the “leak” of the JUST Team transaction ledger on the Internet).

23. CS11 identified “Panprezident1” as a Miami-based broker/reseller affiliated with the JUST Team, involved in facilitating cash-to-cryptocurrency transactions in amounts of approximately \$10,000 to \$300,000. CS11 also identified as photograph of **KULIZHNIKOV** as “Panprezident1.” The “leaked” JUST Team transaction ledger lists approximately thirty-seven

⁵ CS11 is working in hopes of earning sentencing consideration in his/her own case, which involves potential money laundering charges. CS11 has provided agents with extensive intelligence regarding the Target Subjects based on CS11's direct firsthand interactions with them, including fulfilling money laundering contracts for the MLO. The statements made by CS11 have been internally consistent and consistent with statements made throughout different debriefings. CS11's statements also contain extensive detail that I believe could only be obtained through first-hand knowledge and involvement with the Target Subjects, and substantial portions of which agents have been able to corroborate through other means. In sum, I believe CS11 to be reliable.

(37) transactions with “Panprezident1” from approximately March to July 2025, totaling approximately \$1,499,260. The cashiers for all these transactions are identified as either “US:Miami” or “US:Miami-Airplane,” and the “manager” for all the transactions has been identified by both CS7 and CS11 as one of the JUST Team’s managers.

24. Beginning in or around spring 2026, CS10⁶ also identified **KULIZHNIKOV** as a cryptocurrency money launderer servicing drug traffickers, Russian nationals attempting to evade sanctions, and other subjects. CS10 identified @Panprezident1 as one of **KULIZHNIKOV**’s Telegram usernames and [REDACTED] as his phone number. CS10 advised that **KULIZHNIKOV** typically incorporates falsified invoices for business services into his transaction processing. **KULIZHNIKOV** then either remits funds via bank wire transfers from U.S. MTEX GROUP LLC (his U.S.-based company) or other U.S.-based companies controlled by his partners, and/or he conducts bulk cash payouts in exchange for cryptocurrency. CS10 explained that **KULIZHNIKOV** works with a “secret” group and directs multiple cashiers/couriers in Miami, Los Angeles, New York, and elsewhere to facilitate his money laundering activities.

25. CS10 identified several money laundering clients serviced by **KULIZHNIKOV**, including drug traffickers. For example, CS10 identified Sergei RASSOKHIN (“RASSOKHIN”) as a client who was referred to **KULIZHNIKOV** for cryptocurrency money laundering services. RASSOKHIN was previously arrested by Spanish authorities in August 2019 following the seizure

⁶ CS10 is working for monetary compensation, as well as in hopes of earning immigration benefits for a family member. CS10 has provided agents (including me) with extensive intelligence regarding the Target Subjects. The statements made by CS10 have been internally consistent, and consistent with statements made throughout different debriefings. CS10’s statements also contain extensive detail that I believe could only be obtained through first-hand knowledge and involvement with the Target Subjects, and substantial portions of which agents have been able to corroborate through other means (e.g., consensually recorded communications with **KULIZHNIKOV**). In sum, I believe CS10 to be reliable.

of approximately 797 kilograms of cocaine from a U.S.-flagged maritime vessel in international waters.

26. CS10 described a transaction in or around summer 2025 in which **KULIZHNIKOV** received cryptocurrency and coordinated the remittance of approximately \$95,000 bulk currency to a subject in the New York/New Jersey area who had been explicitly introduced to **KULIZHNIKOV** as a drug trafficker involved in procuring fraudulent prescriptions for Oxycontin to be subsequently distributed on the street. To facilitate the money laundering transaction, **KULIZHNIKOV** followed a standard MLO transaction procedure, including establishing a Telegram group chat between the initial broker, the drug trafficking client, **KULIZHNIKOV**'s New York-based cashier/courier, and **KULIZHNIKOV** to coordinate the logistics of the cash delivery.

27. In or around June 2026, agents conducted surveillance of a consensually recorded meeting between CS10 and **KULIZHNIKOV** at a Starbucks in Aventura, Florida. During the meeting, CS10 informed **KULIZHNIKOV** that CS10 was recently contacted by associates in Alexandria, Virginia. CS10 stated, "They sell, of course, white . . . good *kokos* [Russian slang term for cocaine]. They are master of sports [Russian slang to refer to high-level experts] in this business. Many years in this [cocaine] business. They do not use this [cocaine] themselves." CS10 further explained that his/her purported associates in Virginia wanted to convert drug proceeds to cryptocurrency. **KULIZHNIKOV** asked, "How much?" CS10 replied, "Fifty, seventy, one hundred [\$100,000]." **KULIZHNIKOV** agreed to conduct the transaction for a commission of approximately 5.5%. **KULIZHNIKOV** advised CS10 that they would create a group chat "when the transfer [unintelligible] so there is a chain of discussions," **KULIZHNIKOV** would fly to

Virginia, rent a vehicle, and personally pick up the cash, and then he would remit the cryptocurrency within twelve (12) hours.

28. Beginning on or about June 29, 2026, during a consensually recorded Telegram text conversation, CS10 sent a text to **KULIZHNIKOV** at Telegram username @TheAlienEx_manager. CS10 noted that this Telegram account is associated with **KULIZHNIKOV's** business, U.S. MTEX GROUP LLC, and is also used by **KULIZHNIKOV** to coordinate cryptocurrency transactions. CS10 offered a contract to launder cryptocurrency worth approximately \$175,000 to a bank account. CS10 informed **KULIZHNIKOV** the bank account belonged to "this group of my friends from Virginia you and I were talking about at Starbucks." **KULIZHNIKOV** agreed to conduct the transaction for a commission of 2% plus \$100. **KULIZHNIKOV** texted, " $175000 + 2\% + 100 = 178,600$ " and subsequently provided a cryptocurrency address to send the USDT (Tether cryptocurrency).

29. On or about June 30, 2026, agents transferred an initial test of ten (10) USDT from an undercover cryptocurrency wallet address to **KULIZHNIKOV's** address. After **KULIZHNIKOV** confirmed to CS10 that he had received the test transfer, agents transferred the remaining approximately 178,590 USDT to **KULIZHNIKOV's** wallet address. **KULIZHNIKOV** messaged CS10, "Received in full / There will be payments [bank wires] from different companies."

30. Later that day, an undercover bank account located in Fairfax County, Virginia, within the Eastern District of Virginia, received two (2) wire transfers totaling approximately \$85,000 from two U.S.-based bank accounts. On or about July 1, 2026, the undercover bank account received two (2) additional wire transfers totaling approximately \$90,000 from two more U.S.-based bank accounts. The accountholder names for the four bank accounts matched the

businesses that **KULIZHNIKOV** sent CS10 during the Telegram text conversation. **KULIZHNIKOV** requested CS10 provide separate fraudulent invoices for the four wire transfers, listing the details of the sending companies and purporting the transactions to be payments for “marketing services.”

31. In or around August 2026, agents conducted surveillance of a consensually recorded meeting between CS10 and **KULIZHNIKOV** at the Starbucks in Aventura, Florida. During the meeting, CS10 informed **KULIZHNIKOV** that CS10’s associates in Alexandria, Virginia, were ready to conduct an initial test transaction of approximately \$100,000. **KULIZHNIKOV** agreed to pick up the cash on or about August 16, 2026. **KULIZHNIKOV** reiterated that he would charge a 5.5% commission to convert the purported cocaine proceeds to cryptocurrency and would transfer the USDT after he got home [Florida] safely. Shortly after the meeting, **KULIZHNIKOV** sent CS10 a Telegram text message, “Please remind me the city.” CS10 replied, “Alexandria (Virginia).”

32. On or about August 16, 2026, agents coordinated a reverse undercover money laundering operation involving the delivery of approximately \$100,000 bulk cash (purported by CS10 to be cocaine proceeds but actually constituting government funds) by CS10 to **KULIZHNIKOV**. Agents conducted surveillance of the transaction, which was consensually recorded. **KULIZHNIKOV**, after arriving in a rental vehicle, met with CS10 in a public parking lot in Alexandria, Virginia, and sat in CS10’s vehicle. CS10 showed **KULIZHNIKOV** a money counter and offered to let him count the cash to confirm the amount. **KULIZHNIKOV** declined, and they joked about “laying all the money on top of the car and counting it”. CS10 noted that his Alexandria-based associates “couldn’t come over [to meet **KULIZHNIKOV**] because they have just received a large shipment [of cocaine].”

33. On or about August 17, 2026, **KULIZHNIKOV** conducted an initial test transfer of one hundred (100) USDT to an undercover cryptocurrency address provided by CS10 and texted a screenshot of the transaction to CS10. Per agents' instruction, CS10 confirmed that the 100 USDT had been received. **KULIZHNIKOV** promptly transferred approximately 94,400 USDT (i.e., the balance of the payout, less his 5.5% commission) to the undercover cryptocurrency address.

Identification of [REDACTED] as one of KULIZHNIKOV's Brokers

34. In or around 2024, at agents' direction, CS8⁷ negotiated a drug purchase from another co-conspirator affiliated with the JUST Team ("UCC-3") and provided an undercover address in New Jersey (maintained by agents) to receive a portion of the drugs by mail. As partial payment for the drugs, agents transferred approximately \$3,250 from an undercover account to a Zelle⁸ account subscribed to UCC-3. Agents subsequently conducted surveillance of a consensually recorded meeting between CS9⁹ (posing as CS8's courier) and UCC-3's courier in

⁷ CS8 has admitted to past (i.e., over 25 years ago) involvement in racketeering, extortion, arson, drug trafficking, and firearms possession. CS8 also has a prior (i.e., over 25 years ago) conviction for drug trafficking/racketeering pursuant to a prosecution in which CS8 pleaded guilty and testified as a cooperating witness during the criminal trial of a co-defendant. Upon the completion of CS8's prison sentence in that case, CS8 was deported and stopped working with law enforcement. Shortly thereafter (i.e., over 20 years ago), CS8 recanted his/her testimony. Approximately 10 years ago, CS8 began cooperating with law enforcement again, in the hopes of earning immigration benefits and/or financial compensation. CS8 stated that s/he had recanted his/her prior statement in an effort to help his/her co-defendant's family, but that his/her original testimony was truthful. CS8's controlling agents advised me that CS8 has had no negative performance issues during the past 10 years. During this recent cooperation period, CS8 has provided agents (including me) with extensive intelligence regarding the Target Subjects, as well as other drug traffickers and money launderers in other, independent investigations. The statements made by CS8 about the Target Subjects have been internally consistent and consistent with statements made throughout different debriefings. CS8's statements contain extensive detail that I believe could only be obtained through first-hand knowledge and involvement with the Target Subjects, substantial portions of which agents have been able to corroborate through consensual recordings, surveillance, Grand Jury subpoena records, and/or other means.

⁸ Zelle is a digital payment service that allows users to send/receive money through a U.S. bank account by using a mobile application or online banking platform. A user's Zelle account is linked to a bank account with a U.S. mobile number or email address.

⁹ CS9 is working for monetary compensation. CS9 has provided agents with detailed intelligence regarding

Brooklyn, New York. During the meeting, at agents' direction, CS9 delivered an additional \$1,250 in cash to the courier in exchange for approximately 21 grams of cocaine. A parcel containing approximately 57 grams of methamphetamine was also received by agents at the undercover address in New Jersey.

35. In addition to coordinating the distribution of methamphetamine and cocaine, UCC-3 also recommended the MLO's cryptocurrency laundering services to CS8. During a consensually recorded WhatsApp call between CS8 and UCC-3¹⁰ on or about May 15, 2024, CS8 told UCC-3, "I have a [drug] deal taking place in New York, and they are giving me cash. And I need to transfer it to crypto, so can I do it through you?" UCC-3 replied, "I will simply put you in touch, you'll go and give them [the cash], and they will transfer it to crypto in front of you." UCC-3 asked, "What is the amount?" CS8 replied, "Between about sixty [\$60,000], maybe eighty [\$80,000]." UCC-3 confirmed, "This is without problems, no problems." UCC-3 offered, "If you want, I can directly connect you with her, with the girl [REDACTED] . . . They have an office in New York and Los Angeles but live in Miami."

36. I have reviewed a consensually recorded WhatsApp text conversation with UCC-3 (using a WhatsApp account associated with phone number [REDACTED]), which SA Savvides extracted from CS8's phone. Records provided by T-Mobile confirmed the x[REDACTED] phone number was subscribed to UCC-3. The WhatsApp extraction shows the time/length of the above-

the Target Subjects. The statements made by CS9 have been internally consistent and consistent with statements made throughout different debriefings. CS9's statements also contain details that I believe could only be obtained through first-hand knowledge and involvement with the Target Subjects, and substantial portions of which agents have been able to corroborate through other means (e.g., consensually recorded communications with **KULIZHNIKOV**). In sum, I believe CS9 to be reliable.

¹⁰ In or around April 2025, UCC-3 was arrested in Hawthorne, California, pursuant to a California state arrest/search warrant and the seizure of four firearms. UCC-3 was subsequently convicted in the Central District of California on charges of 18 U.S.C. § 922(g)(5) (Alien in Possession of a Firearm). I have spoken with SA Zachary Savvides, who was present during two separate post-arrest interviews of UCC-3 in 2025 and heard him speak at length. SA Savvides recognizes UCC-3's voice in this recorded call.

referenced recorded call on or about May 15, 2024, in which UCC-3 offered to introduce CS8 to

██████████. Approximately five minutes after the call, UCC-3 texted a contact card for ██████████” [██████████] with phone number ██████████.

- a. Records provided by Apple in response to an order obtained in June 2026 pursuant to 18 U.S.C. § 2703(d) demonstrate the x ██████████ phone is linked to an Apple account in the name of ██████████. Records provided by JPMorgan Chase Bank pursuant to legal process also show that the x ██████████ phone is linked to a bank account owned by ██████████.

37. On or about May 16, 2024 (i.e., the day after UCC-3 sent ██████████ contact card), CS8 sent a text message to ██████████ at a WhatsApp account associated with the x ██████████ phone. I have reviewed this consensually recorded WhatsApp text conversation, which SA Savvides extracted from CS8’s phone. During the conversation, CS8 stated, “Hello ██████████. It’s [CS8] from [UCC-3], what time is good for you to talk?”

38. Shortly thereafter, during a consensually recorded call between ██████████ and CS8, ██████████ agreed to remit cryptocurrency in exchange for bulk drug proceeds delivered in New York. CS8 explained that s/he has “access to this powder [cocaine], so I’m straight from the Dominican Republic . . . close to the border with Colombia.” CS8 further explained that cocaine costs \$10 per bag in the Dominican Republic for “so-so” [mid-range purity] but that for “\$12, it’s just, well – it’s unreal – scraping it off [the wholesale cocaine brick] with a knife in front of you.” CS8 further explained, “It’s easier to get it [cocaine] to New York. Because there’s a very large Dominican community, and they’re dragging [importing] it there.”

39. During the May 2024 consensually recorded call, CS8 inquired about the MLO’s transaction procedures. CS8 noted, “[UCC-3] explained it to me that I will come to you, sit down,

you will send it [cryptocurrency], and I will give you the [cash] money.” [REDACTED] confirmed, “You’ll simply give a [cryptocurrency] wallet, and we would transfer it [cryptocurrency] into it, and that’s it. The wallet can be Coinbase [cryptocurrency exchange] or somewhere; it is not that important.” [REDACTED] explained, “We usually meet in the car.” [REDACTED] explained further, “A person [cashier/courier] will take it, immediately count it, and at the same moment as he counts, he transfers [the cryptocurrency].” [REDACTED] assured CS8, “We don’t even have the opportunity to deceive in any way [shortchange the payout], because in the car – in the parking lot, that is – there is some kind of option [to reconcile any difference between the cash payment and cryptocurrency payout].”

40. During the May 2024 consensually recorded call, [REDACTED] also described how the MLO operates throughout the United States and other countries. [REDACTED] stated, “I need to see if there is a person [cashier/courier] in New York. And if he is there, there will probably be a slightly higher percentage [commission rate] than in Miami.” [REDACTED] estimated the commission would be approximately 3% in Miami and 4 to 4.5% in New York. [REDACTED] explained, “Usually it is always possible [to deliver bulk cash to a cashier] in Miami. Soon it will also be possible in Los Angeles. New York – not always. And regarding services, we are able to transfer [cryptocurrency] for you, and we can also give it in cash. That is, if you are interested, for example, in giving cash here [in the United States] and having it given to you in Russia, then this can also be done in real time.” [REDACTED] added, “Soon there will be an opportunity to have this done in Dubai . . . but in Dubai, it can be transferred usually with crypto. That is, in Russia, there is just demand to give in cash and receive cash here [in the United States]. And in Dubai, it is quite easy to transfer in crypto.”

41. On or about June 22, 2024, during a consensually recorded WhatsApp text conversation, CS8 asked [REDACTED] “Could we make the first transfer on Wednesday [June 26, 2024] morning? I’m supposed to receive cash on Wednesday morning, and I’d like to transfer it right away.” [REDACTED] replied, “Yes, no problem.”

42. On or about June 24, 2024, CS8 was invited to a Telegram group chat entitled “Order CSH-1010-MIA.” This notation follows the MLO’s standard contract registration format—consistent with the format of transactions documented on the “leaked” JUST Team transaction ledger, as well as transactions referenced in the consensually downloaded Telegram chats with UCC-1. The June 2024 group participants included [REDACTED] MT//EX [i.e., U.S. MTEX GROUP LLC, **KULIZHNIKOV**’s front business], and “Cashier Nikolai MT//EX,” used by an additional co-conspirator (“UCC-4”). The group administrator confirmed the transaction details, “The client receives: 50 000.0 USDT / City: MIA.” [REDACTED] also sent CS8 a private Telegram text (using Telegram username @[REDACTED], linked to the x[REDACTED] phone), stating, “Hello! We’ve created a group where we can discuss all the logistical details . . . I won’t be able to meet tomorrow, but I can call for now.” CS10 has also identified UCC-4 as a cashier/courier who, prior to UCC-4’s arrest in an unrelated investigation, regularly delivered bulk currency payouts to clients on behalf of **KULIZHNIKOV**.

43. On or about June 26, 2024, agents coordinated the delivery of approximately \$50,000 in bulk cash (purported to be drug proceeds, but actually constituting government funds) by CS8 to their ([REDACTED] and **KULIZHNIKOV**’s) cashier/courier (subsequently identified as UCC-4) in a parking lot in Aventura, Florida. Agents conducted surveillance of the meeting, which was consensually recorded. During the meeting, UCC-4 brought a money counter and counted the cash in CS8’s vehicle. Shortly thereafter, an undercover cryptocurrency wallet

address (provided by CS8 but controlled by agents) received two (2) incoming transfers totaling the payout sum (i.e., after the MLO deducted a 5% commission) of approximately 47,500 USDT (Tether cryptocurrency).

44. The following day (on or about June 27, 2024), CS8 met with [REDACTED] in Sunny Isles, Florida. Agents conducted surveillance at the meeting, which was consensually recorded. During the meeting, CS8 reiterated that CS8 trusted [REDACTED] because “[UCC-3] recommended you to me.” CS8 expressed concern that the cashier/courier [UCC-4] who picked up the cash the previous day had indicated that he did not even know [REDACTED]. [REDACTED] replied, “I have partners, these people know me . . . I’ll just explain it to you. Look, drug dealers, they all know--we’re in this kind of business where reputation is important, I suppose, isn’t it?” [REDACTED] further explained, “The less they [cashiers/couriers] know me there, the better. This is the business I built this way. It’s like a cashier, and a cashier is like an ATM, they only dispense.”

45. During the June 27, 2024, consensually recorded meeting, [REDACTED] also reiterated that the commission for transactions conducted in New York would be higher than in Miami, describing how they leveraged different MLO teams to fulfill contracts outside their individual market(s) and expand their overall operating scale. [REDACTED] explained, “In New York, the percentage is somewhere around eight [8%], because we cooperate with another company there . . . it’s an extra link in the chain. This is a kind of business that is difficult to do in other cities, because it’s very important to have someone you can hold accountable if anything happens. Who lives there, that someone knows – some type of cashiers. If it’s New York, it’s very difficult to manage from afar. That’s why we have a local operation, locally here [in Miami], and we also have a local operation in L.A. In New York, we don’t have a personal [manager on site to

supervise cashiers].” [REDACTED] described one of the MLO’s standard transaction procedures (which they had also used during the June 26, 2024, transaction): “When we do this, we create a Telegram group. I’m in this group, there are our partners there [New York]; we message each other.” CS8 asked, “Can you tell me that your partner is trustworthy?” [REDACTED] confirmed that her partner is Russian and reassured CS8, “He is definitely trustworthy.”

46. From in or around July 2024 through in or around September 2025, agents coordinated a series of eleven (11) reverse undercover money laundering operations directly brokered by **KULIZHNIKOV** and involving the delivery of bulk cash (purported to be drug proceeds, but actually constituting government funds) by CS8 and/or CS9 (posing as CS8’s courier) in various cities across the United States. Agents conducted surveillance of each of these transactions, which were all consensually recorded. The Target Subjects adhered to the standard transaction procedures they had previously described. Namely, a representative of the MLO (typically a cashier/courier, such as UCC-4) would meet the CSs in a parking lot, the cashier/courier would get into the undercover vehicle (sometimes personally confirming the amount with a money counter), and the corresponding cryptocurrency payout sum, less a commission, would be promptly transferred to an undercover cryptocurrency wallet address (provided by CS8 but controlled by agents). In each of the transactions, an initial transfer of ten (10) or one hundred (100) USDT was sent first, followed by the payout balance. Specifically:

- a. Approximately \$50,000 was delivered to an MLO cashier/courier by CS8 on or about July 22, 2024, in Brooklyn, New York, in exchange for 46,250 USDT;
 - i. The same wallet address that sent the cryptocurrency in the above-referenced June 26, 2024, transaction (directly coordinated by

[REDACTED] was also used to send the cryptocurrency to the undercover wallet address in this transaction (directly coordinated by **KULIZHNIKOV**).

- b. Approximately \$50,000 was delivered to an MLO cashier/courier by CS8 on or about August 21, 2024, in Brooklyn, New York, in exchange for 46,500 USDT;
- c. Approximately \$50,000 was delivered to an MLO cashier/courier by CS8 on or about September 19, 2024, in Brooklyn, New York, in exchange for 46,360 USDT;
- d. Approximately \$100,000 was delivered to UCC-4 by CS8 on or about November 12, 2024, in Sunny Isles Beach, Florida, in exchange for 94,500 USDT;
 - i. During this transaction, CS8 asked, “Who should I send the code to?” CS8 clarified, “The [cryptocurrency] wallet.” UCC-4 confirmed “Pasha, Pasha [nickname for Pavel] . . . Everything is through Pavel [KULIZHNIKOV].”
- e. Approximately \$200,000 was delivered to an MLO cashier/courier (“UCC-5”) by CS8 on or about December 11, 2024, in Hallandale Beach, Florida, in exchange for 189,000 USDT;
 - i. As described below, UCC-5 was observed following two reverse undercover money laundering transactions conducted with [REDACTED] and receiving cash from him in or around summer 2024.
- f. Approximately \$150,000 was delivered to UCC-4 by CS8 and CS9 on or about February 4, 2025, in Aventura, Florida, in exchange for 141,750 USDT;

- g. Approximately \$200,000 was delivered to UCC-4 by CS8 and CS9 on or about March 11, 2025, in Hollywood, Florida, in exchange for 189,000 USDT;
- h. Approximately \$150,000 was delivered to an MLO courier by CS9 on or about April 22, 2025, in Queens, New York, in exchange for 139,050 USDT;
- i. Approximately \$150,000 was delivered to **KULIZHNIKOV** by CS8 and CS9 on or about June 24, 2025, in Hallandale Beach, Florida, in exchange for 141,750 USDT;
- j. Approximately \$150,000 was delivered to **KULIZHNIKOV** by CS9 on or about August 20, 2025, in Hallandale Beach in exchange for 141,750 USDT; and
- k. Approximately \$200,000 was delivered to **KULIZHNIKOV** by CS8 on or about September 30, 2025, in Dania Beach, Florida in exchange for 189,000 USDT.

47. During the September 19, 2024, transaction in New York, CS8 commented, “They don’t want to transport money from here [New York] to there [Miami].” The MLO cashier/courier asked, “To be handed out in Miami?” The MLO cashier/courier explained the potential risk of law enforcement seizing the bulk cash during a vehicle stop when driving from New York to Miami—and that vehicles had been stopped previously. The MLO cashier/courier stated, “They’re a little scared there, you know, to transport it [by car]. It’s easier by plane. In Miami, in Georgia, you drive by car, they [police] stop you.” When CS8 expressed surprise that law enforcement would know which vehicle to stop, the cashier/courier replied, “Somehow, they can detect it in the car, I don’t know. I hear a car got busted there, a car got busted there.” CS8 indicated this risk is therefore

factored into the price, stating, “Believe me, the cars that carry it [bulk cash] . . . there’s a price difference. That’s the Miami price.”

- a. In my training and experience, I know that driving routes from New York to Miami would most likely transit the Eastern District of Virginia.
- b. As detailed above, during the August 16, 2026, reverse undercover money laundering transaction, **KULIZHNIKOV** indicated to CS10 that he planned to drive the bulk cash from Alexandria, Virginia, to Miami. However, **KULIZHNIKOV’s** commission during this transaction (5.5%) was significantly higher than the commission (2% plus \$100) he charged during the June 2026 reverse undercover money laundering transaction (which did not involve transporting bulk cash long distances).
- c. CS10 also stated that **KULIZHNIKOV** has described renting a vehicle and driving outside Florida to pick up bulk cash from the MLO. **KULIZHNIKOV** further described instances in which MLO members were stopped by law enforcement while transporting bulk cash and the funds were seized. MLO members made no effort to file claims regarding the seized funds.

48. Although **KULIZHNIKOV** managed these transactions, [REDACTED] continued facilitating logistics and communication. For example, on or about July 3, 2024, during a consensually recorded Telegram conversation, [REDACTED] sent a Telegram text to CS8 and **KULIZHNIKOV** (using the @Panprezident1 account). [REDACTED] texted, “[CS8 name], meet my partner, Pasha [nickname for Pavel; **KULIZHNIKOV**]. You can handle all your business with him. Pasha will be happy to help you with New York and transfers from Russia.” **KULIZHNIKOV** texted, “Nice to meet you.” CS8 replied, “Hello Pasha. I’ll know the time and

day for the transfer later. I'll let you know." Agents subsequently commenced this series of 11 transactions (detailed above) with the delivery of approximately \$50,000 to **KULIZHNIKOV's** cashier/courier in Brooklyn, New York on or about July 22, 2024.

49. On or about January 14, 2025, following the completion of the three transactions involving bulk cash deliveries in Brooklyn (along with three bulk cash deliveries in the Miami area), remitted as USDT cryptocurrency, [REDACTED] sent CS8 a text to solicit additional transactions. During a consensually recorded Telegram conversation, [REDACTED] stated, "Hello! I'd like to remind you that in New York, this is a brokerage You've already worked with them, and everything went smoothly though, so there's no reason to think anything could go wrong."

50. During the last three undercover transactions in this series, **KULIZHNIKOV** personally picked up the bulk currency and coordinated the USDT transfers to the undercover cryptocurrency addresses. In each of these three undercover transactions, upon receiving the cash, **KULIZHNIKOV** promptly coordinated an initial test transfer of 100 USDT followed by the balance of the payout, less his commission, to an undercover cryptocurrency address. The CSs contacted an undercover agent to confirm receipt of the USDT before **KULIZHNIKOV** departed the meeting. During the June 24, 2025, transaction, **KULIZHNIKOV** explained that he was personally conducting his cash pickups now, since two of his cashiers had stolen money recently. When CS8 inquired how much the first cashier had stolen, **KULIZHNIKOV** replied, "A million [\$1 million]." **KULIZHNIKOV** complained, "Because of this, I'm having such a hassle." **KULIZHNIKOV** further explained, "I have another one [cashier/courier] here, another so-called buddy who also left with fifty [\$50,000]." CS8 expressed concern about conducting future money laundering transactions in other cities (i.e., where **KULIZHNIKOV** may not be able to personally

pick up the cash), stating, “Pash [nickname for Pavel], I beg you, I don’t want to go through strangers.” **KULIZHNIKOV** reassured CS8, “If I do it [accept a money laundering contract], I guarantee it [payout].”

- a. CS10 also advised that in or about summer 2025, both **KULIZHNIKOV** and UCC-4 discussed how one of **KULIZHNIKOV**’s cashier/couriers had stolen money intended for delivery to one of **KULIZHNIKOV**’s clients. CS10 noted that **KULIZHNIKOV** personally covered this loss after the cashier/courier disappeared.

51. **KULIZHNIKOV** also discussed UCC-3’s recent arrest during these final three transactions. **KULIZHNIKOV** acknowledged the MLO’s heavy dependence upon electronic communication to coordinate their money laundering operations. **KULIZHNIKOV** also indicated that [REDACTED] and he were concerned about their potential exposure to law enforcement.

- a. During the transaction on or about June 24, 2025 (i.e., approximately two months after UCC-3’s arrest in California on firearms charges), CS8 confirmed, “[UCC-3] is locked up [imprisoned]. They caught him over a weapon.” **KULIZHNIKOV** asked, “A combat weapon?” CS8 replied, “I think so . . . well, he shot in a club . . . and they came to his house [unintelligible] machine gun, pistol, rifle. Well anyway, he’s locked up. He will not get out.” **KULIZHNIKOV** noted, “I also talked to him [UCC-3] on the phone.”
- b. During the September 30, 2025, transaction, **KULIZHNIKOV** commented, “Also our female friend [REDACTED] was inquiring – she is very worried.” CS8 acknowledged, “Yes. But he [UCC-3] is in big trouble.” **KULIZHNIKOV** stated, “This is because of the shooting.” CS8 replied, “First

of all, because of the shooting. Secondly, a weapon was found on him. Third, they are pinning drugs on him.” CS8 suggested the police had interviewed UCC-3, stating, “They [police] asked with whom and whether he has financial exchanges with someone in Miami.” CS8 asked, “How do they [police] know the information? I say, how can they know? Well, he [UCC-3] has it on the phone.” **KULIZHNIKOV** agreed, stating, “In my opinion.” As they continued discussing UCC-3’s arrest and speculated about their possible exposure to law enforcement as a result, **KULIZHNIKOV** cautioned, “You have to be careful.”

52. As described further above, [REDACTED] has explicitly described her preference to coordinate money laundering transactions with **KULIZHNIKOV** via the encrypted Telegram application (“when we do this, we create a Telegram group – I’m in this group, there are our partners there; we message each other”). The reverse undercover money laundering transactions involving [REDACTED] (when CS8 was invited into a Telegram chat with **KULIZHNIKOV** and [REDACTED] reaffirmed this. However, pen register data and toll records demonstrate that throughout the investigation, she has also remained in phone contact with **KULIZHNIKOV**’s brother—whom **KULIZHNIKOV** has stated is also involved in their money laundering operations. In or around June 2026, CS10 also identified **KULIZHNIKOV**’s brother and advised that CS10 believes **KULIZHNIKOV**’s brother assists with cryptocurrency money laundering operations.

- a. As described above, during the May 2024 consensually recorded call, [REDACTED] described the MLO’s operations in various cities and commented, “Soon it will also be possible in Los Angeles.”

b. Later, during the consensually recorded June 24, 2025, reverse undercover money laundering transaction in Florida, **KULIZHNIKOV** emphasized the importance of having trustworthy cashier/couriers (detailed further above). **KULIZHNIKOV** noted, “I have Kolia [nickname for both UCC-4 and UCC-5], too. Kolia is here.” CS8 then inquired about the possibility of conducting future money laundering transactions in Los Angeles. **KULIZHNIKOV** replied, “I actually have a brother there . . . he can help me with that.” CS8 replied, “Brother? Or relative?” **KULIZHNIKOV** reassured CS8, “My own brother If I do it [accept a money laundering contract], I guarantee it [payout].” CS8 inquired about the commission rate, and **KULIZHNIKOV** replied, “It will be approximately the same as New York. Between Miami and New York.”

53. Pen register data and toll records for the period July 1, 2026 through August 12, 2026 show there were four (4) contacts between a phone number listed in CBP records as belonging to **KULIZHNIKOV**’s brother and [REDACTED] x [REDACTED] phone. During the same period, there were an additional twelve (12) contacts between **KULIZHNIKOV**’s brother and phone number [REDACTED]. CBP records show the x [REDACTED] phone is another contact number for [REDACTED] and records produced by PayPal also list the x [REDACTED] phone as a contact (along with the x [REDACTED] phone) for a Venmo account subscribed to [REDACTED]

Analysis of KULIZHNIKOV’s Cryptocurrency Addresses

54. Open-source blockchain analysis on Tronscan,¹¹ records provided by Bybit (a centralized cryptocurrency exchange) for an account registered to “**PAVEL ALEKSEYEVICH**

¹¹ Many different blockchains can be used to send and receive cryptocurrency. A blockchain is a shared, secure, and decentralized digital ledger that records transactions across many computers, creating a

KULIZHNIKOV” (and listing **KULIZHNIKOV**’s date of birth), and other evidence have led to the identification of at least forty-three (43) addresses directly associated with **KULIZHNIKOV**. Based on my training and experience, I know that sophisticated money launderers frequently change cryptocurrency addresses in the effort to elude detection by law enforcement. Additionally:

- a. Ten (10) of those addresses were used to remit the payouts in the fourteen (14) reverse undercover money laundering transactions brokered by [REDACTED] and **KULIZHNIKOV** from June 26, 2024, to August 17, 2026 (described above).
- b. As noted above, the same address was used to conduct the payouts in both the June 26, 2024, transaction (brokered directly by [REDACTED] in the Miami area and the July 22, 2024, transaction (brokered by **KULIZHNIKOV**) in New York. This address also received funds directly from the Bybit account registered to **KULIZHNIKOV**.
- c. Similarly, a second address was used to conduct the payouts in the August 21, 2024, and September 19, 2024, undercover transactions brokered by **KULIZHNIKOV**. This address also received funds directly from the Bybit account registered to **KULIZHNIKOV**.

transparent, tamper-proof history. All the undercover cryptocurrency transactions involving **KULIZHNIKOV**, [REDACTED] and [REDACTED] referenced herein were conducted with USDT on the TRON blockchain. The TRON blockchain is a global leader for stablecoin transfers, particularly USDT. It has hundreds of millions of user accounts and a high transaction activity. It is estimated that the TRON blockchain processes approximately 11 million transactions daily worth over \$22 billion. It has been identified by the United Nations Office on Drugs and Crime, and others, as a preferred choice for cryptocurrency money launderers. Tronscan is a reliable means for viewing the TRON blockchain because it is the official explorer for the Tron blockchain. It offers real-time, transparent access to all the public data on the blockchain.

- d. A third address was used to conduct the payouts of three undercover transactions: November 12, 2024; December 11, 2024; and February 4, 2025. As noted above, UCC-4 confirmed during the November 12, 2024, transaction that **KULIZHNIKOV** controlled this wallet address (“everything is through Pavel”).
- e. A fourth address was used to conduct the payout in the April 22, 2025, undercover transaction brokered by **KULIZHNIKOV**. This address also received funds directly from the Bybit account registered to **KULIZHNIKOV**.
- f. The ten addresses (10) used to conduct the payouts in the fourteen (14) undercover transactions brokered by [REDACTED] and **KULIZHNIKOV** processed a total transaction volume of over \$71 million from in or around April 2022 to August 2026.

Identification of [REDACTED] as Another MLO Cashier/Courier

55. Beginning in or around late 2023, CS13¹² identified an unindicted co-conspirator (“UCC-6”) as a money launderer who coordinated the receipt of bulk cash in numerous countries and corresponding remittance of USDT. During a series of consensually recorded negotiations, CS13 informed UCC-6, in sum and substance, that CS13 laundered bulk cocaine proceeds in the United States and other countries on behalf of Clan del Golfo and the Sinaloa Cartel.

¹² CS13 is working for monetary compensation and has provided agents with extensive intelligence regarding the Target Subjects, as well as other drug traffickers and money launderers in other, independent investigations. The statements made by CS13 have been internally consistent, and consistent with statements made throughout different debriefings. CS13's statements also contain extensive detail that I believe could only be obtained through first-hand knowledge and involvement with the Target Subjects, and substantial portions of which agents have been able to corroborate through other means (e.g., consensually recorded conversations with [REDACTED]). In sum, I believe CS13 to be reliable.

56. For example, during a consensually recorded meeting with UCC-6 in or around late 2023, CS13 stated, “I do a lot of work with the Gulf Cartel of Colombia [Clan del Golfo]. I make pickups, cash in the northern part of the United States and the eastern part. That’s Boston, New York, Atlanta, and Florida. And then with the Sinaloa Cartel in Mexico, I do the West Coast – L.A. and so forth.” CS13 offered, “This particular group is beginning to ship a few kilos [kilograms of cocaine] to Belgium and the Netherlands.” CS13 solicited UCC-6’s assistance with laundering bulk drug proceeds to USDT (Tether cryptocurrency), stating that CS13 was unable to process large sums or receive bulk cash in Europe. CS13 explained, “One of the guys in Sinaloa [Cartel] told me, ‘Oh, I got \$12 million dollars up there to pick up. I cannot handle that.’” CS13 further stated, “I’ve been working with a guy in Bogota He just moved about \$36, 40 million dollars in about two months for a group in the Colombian plains. That’s the eastern part of Colombia in the jungle They’re cultivating so much coke. It’s amazing. And they’re shipping thousands and thousands of kilos.”

57. UCC-6 assured CS13, “I work with the biggest guy in Europe, and he can do USDT, and he can pick up all over.” UCC-6 also specifically noted, “I spoke to him as well about the U.S. He has an operation over there . . . a reliable set-up there that he works. Already. In the major cities.” During subsequent, consensually recorded conversations between CS13 and UCC-6 (primarily over Telegram), UCC-6 informed CS13 that UCC-6’s partner had agreed to launder bulk cash proceeds to USDT cryptocurrency on behalf of CS13. UCC-6 instructed CS13 to relay all the transaction details (e.g., contract amount, time and location for delivering the cash proceeds, cryptocurrency wallet addresses to receive the USDT) directly with UCC-6. UCC-6 advised that UCC-6 would forward the transaction details to UCC-6’s partner, UCC-6’s partner would then dispatch a cashier/courier to pick up the bulk currency from CS13, and UCC-6’s partner would

then complete the USDT cryptocurrency payout (less a commission for UCC-6 and the partner). UCC-6 offered to conduct transactions in amounts up to \$3 million.

58. On or about June 13, 2024, and July 16, 2024, agents coordinated two (2) reverse undercover money laundering operations directly brokered by UCC-6 and involving the delivery of bulk cash (purported to be drug proceeds, but actually constituting government funds) by CS13 in the Miami area. Agents conducted surveillance of these transactions, which were both consensually recorded. In each of the transactions, [REDACTED] was the cashier/courier dispatched by the MLO to meet CS13 in a hotel lobby and pick up the bulk cash. For each transaction, [REDACTED] provided CS13 with a token (a \$1 banknote, the serial number of which had previously been provided by UCC to CS13, used as a code and receipt for the cash transfer). The corresponding USDT payouts, less a commission of approximately 5%, were transferred to the undercover wallet addresses shortly after the cash deliveries.

59. Following the June 2024 delivery of \$325,000 bulk currency by CS13 to [REDACTED] agents observed [REDACTED] drive to a condo complex in the Brickell neighborhood in Miami. Agents observed UCC-5 get into the passenger seat of [REDACTED] vehicle and count money on the front dash. Shortly thereafter, UCC-5 exited [REDACTED] vehicle, holding what appeared to be a bulk amount of cash in his hand, and departed the area in another vehicle. That same day, a total of approximately 308,056 USDT was received in the undercover wallet addresses CS13 had provided to UCC-6.

- a. As described above, UCC-5 was the cashier/courier who picked up approximately \$200,000 bulk currency from CS8 in Hallandale Beach, Florida, on or about December 11, 2024, as part of the sixth reverse undercover money laundering transaction brokered by **KULIZHNIKOV** and [REDACTED]

60. The day before the July 2024 delivery of approximately \$330,000 bulk currency by CS13 to [REDACTED] CS13 asked UCC-6 via Telegram text, “Will I see the same guy [REDACTED] UCC-6 replied, “That will be news tomorrow, but exact same procedure.” The following day, UCC-6 forwarded a screenshot of a message from UCC-6’s partner to CS13 via Telegram text. In the message, UCC-6’s partner confirmed, “It’s the same man from previous time.” The screenshot also depicted a photo of the token (a \$1 banknote). Shortly thereafter, [REDACTED] arrived at the hotel lobby. CS13 handed over the cash (approximately \$330,000), and [REDACTED] provided the token. CS13 then spoke with UCC-6 during a consensually recorded phone call. CS13 commented that CS13 had just met with the same courier. UCC-6 replied that it will always be the same courier [REDACTED]

61. Agents observed [REDACTED] depart the July 2024 meeting and drive to 1008 NE 10th Street, Hallandale Beach, Florida. CBP records list a particular apartment in this complex as UCC-5’s residence. [REDACTED] walked into the apartment complex with a black backpack. Shortly thereafter, agents observed [REDACTED] return to his vehicle with the black backpack and depart the area. A couple hours later, agents followed [REDACTED] to a restaurant and observed UCC-5’s vehicle parked in the lot. UCC-5 got in the passenger seat of [REDACTED] vehicle. Shortly thereafter, UCC-5 exited [REDACTED] vehicle with a white bag and departed the area in his car. That same day, a total of approximately 312,800 USDT was received in the undercover wallet address CS13 had provided to UCC-6.

- a. Based on my training and experience, based on my knowledge of this investigation and based on UCC-5’s role as a cashier/courier in the December 11, 2024, undercover transaction brokered by **KULIZHNIKOV**, I believe [REDACTED] transferred at least a portion of the bulk currency delivered by

CS13 in the June 2024 and July 2024 transactions to UCC-5 for further processing by the MLO and/or delivery to other clients who had purchased U.S. dollars with cryptocurrency.

62. Agents conducted surveillance of [REDACTED] on multiple occasions in November 2025 and January 2026, observing him conduct similar meetings with other subjects in a public parking lot located a short distance (i.e., approximately one mile) from his residence. Based on my training and experience, I know that money launderers commonly select public parking lots near their residences and other stash locations (i.e., where bulk currency is counted, processed, and stored) to meet clients. I also know that money launderers commonly offer to count bulk currency together with the client at the time of the transfer, to ensure both parties agree on the amount that has been delivered. As detailed herein, the couriers/clients have discussed and/or actually counted the cash during many of the undercover transactions. If a portable money counter is not available in their vehicles, this count may take place in a stash house location. During the November 2025 and January 2026 surveillances, agents observed [REDACTED] conduct meetings with numerous subjects in the same public parking and either transfer cash and/or drive them back to his residence for a brief period of time (i.e., consistent with the time it would take to count a bag containing bulk currency) before returning them to their vehicles at the public parking lot.

- a. For example, on November 6, 2025, surveillance observed [REDACTED] drive from his residence to the public parking lot. [REDACTED] pulled into the lot, immediately turned around, and returned to his residence. Approximately two hours later, [REDACTED] returned to the same public parking lot. [REDACTED] parked in the lot, got into the front passenger seat

of Vehicle #1 and exited a few minutes later. [REDACTED] then met with another subject in Vehicle #2 and handed over what appeared to be an unknown amount of cash. Surveillance observed the Vehicle #2 driver counting the cash by hand. [REDACTED] was also observed meeting the Vehicle #2 driver again during surveillance conducted on January 6, 2026.

- b. On November 12, 2025, surveillance observed [REDACTED] drive to the same public parking lot and park behind Vehicle #3. The Vehicle #3 driver, carrying an orange bag, approached [REDACTED] and shook hands with him through [REDACTED] window. The Vehicle #3 driver got into [REDACTED] vehicle and went back to [REDACTED] residence. [REDACTED] and the Vehicle #3 driver (still carrying an orange bag) walked inside. Shortly thereafter, [REDACTED] and the Vehicle #3 driver exited, and [REDACTED] drove the Vehicle #3 driver back to the public parking lot.
- c. On January 6, 2025, prior to meeting with the Vehicle #2 driver, surveillance observed [REDACTED] meet with a subject in Vehicle #4 in the same public parking lot. [REDACTED] and the Vehicle #4 driver returned to [REDACTED] residence. A few minutes later, [REDACTED] and the Vehicle #4 driver exited, and [REDACTED] drove the Vehicle #4 driver back to the public parking lot.

63. WhatsApp pen register data also demonstrates [REDACTED] routinely interacts with other money launderers and/or money laundering clients. For example, during April 2024, pen register data shows 143 contacts between a WhatsApp account associated with [REDACTED] and an account associated with [REDACTED]. The x [REDACTED] phone was registered to “[REDACTED]

██████████ during this period, and CBP records also identify it as used by ██████████. The x██████████ number was previously identified as a money laundering courier in an independent DEA investigation.

- a. Specifically, in early 2024, agents conducted a reverse undercover money laundering transaction coordinated by an independent money laundering broker and involving the delivery of bulk cash (i.e., over \$100,000) to a courier in the U.S. During the negotiations, the independent broker provided a token number for the cash transfer. An undercover officer was subsequently contacted by a coordinator, who provided the token number and identified the x██████████ phone as their courier.

64. Bank records provided by JP Morgan Chase for an account registered to U.S. MTEX GROUP LLC (i.e., **KULIZHNIKOV**'s business) show five (5) Zelle payments from ██████████ during the period in or around April 2024 to November 2024.

65. Subscriber/toll records demonstrate there were eighty (80) contacts between **KULIZHNIKOV**'s x██████████ phone and ██████████ x██████████ phone in or around May 2024 through August 2024 (i.e., contemporaneous with the two undercover cash deliveries to ██████████). ██████████ x██████████ phone was subsequently suspended for non-payment.

66. Toll records further demonstrate that during the same period (May 2024 through August 2024, contemporaneous with the two undercover cash deliveries to ██████████) there were seventy-one (71) additional contacts between **KULIZHNIKOV**'s x██████████ phone and ██████████. Subscriber records demonstrate the subscriber name on the account for the x██████████ phone is ██████████ wife, who is also listed as the registered owner of the vehicle that

██████████ drove to pick up bulk cash from CS13 during both undercover money laundering transactions in June 2024 and July 2024.

67. Pen register data and toll records for June 2024 through July 2026 (when ██████████ x ██████████ phone was suspended for non-payment) show a total of 258 contacts between **KULIZHNIKOV**'s x ██████████ phone and ██████████ x ██████████ phone. Throughout this period, ██████████ was one of **KULIZHNIKOV**'s most frequent contacts. Based on my training and experience, based on my knowledge of the Target Subjects, based on ██████████ delivery of cash to another one of **KULIZHNIKOV**'s couriers (UCC-5) after both undercover cash deliveries to him by CS13, and based on the high volume of contacts between ██████████ and **KULIZHNIKOV**, I believe ██████████ is a regular cashier/courier for **KULIZHNIKOV** and the MLO.

68. Based on my training and experience, and based on the evidence generated in this investigation, I know that cashier/couriers play an integral role in the operation of an illicit money services business. The cashier/courier serves as the MLO's physical representative to its clientele (i.e., the face of the business). As UCC-1 previously explained (detailed above), a cashier/courier may even sometimes serve as a manager's "representative" during in-person negotiations (i.e., if the manager is located in a different country). As **KULIZHNIKOV** has also emphasized, the MLO does not entrust this responsibility lightly. Indeed, **KULIZHNIKOV** has learned through personal experience (detailed further above) that an unreliable cashier/courier can result in substantial financial losses (i.e., if the cashier/courier steals a large sum of bulk cash).

69. Conversely, a trusted and experienced cashier/courier increases the entire MLO's operating scale. As ██████████ has discussed, the MLO recognizes the risk of law enforcement exposure faced by cashier/couriers and intentionally compartmentalizes contacts

between members to minimize that exposure ("this is the business I built"). Thus, a particular manager need not personally meet every individual cashier/courier – provided the cashier/couriers have been vetted by another MLO manager. For example, [REDACTED] did not need to personally meet UCC-4 before he picked up the cash in the June 26, 2024, transaction she brokered, since he had been vetted by **KULIZHNIKOV** ("reputation is important"). UCC-6 also reiterated this point when (as described above) he assured CS13 that the cashier/courier for their transactions would always be [REDACTED]. Trusted, reliable cashier/couriers often earn a regular commission based on the volume of bulk cash they are responsible for processing. For example, CS10 advised that **KULIZHNIKOV**'s cashier/couriers typically earn a commission rate of 0.3% to 0.5% and are paid in cash.

70. Certified Bank Secrecy Act records provided by the Financial Crimes Enforcement Network ("FinCEN") confirm that no **FinCEN** Form 107 (Registration of Money Services Business) was filed by or on behalf of [REDACTED] for the period January 2020 through on or about August 10, 2026. Similarly, no such forms for this period were filed by or on behalf of **KULIZHNIKOV**, his business (U.S. MTEX GROUP LLC), or [REDACTED]

CONCLUSION

71. In sum, the investigation has demonstrated that **KULIZHNIKOV**, [REDACTED] and their co-conspirators in the MLO have achieved a vast money laundering capacity by developing an international network of managers and cashiers/couriers (e.g., [REDACTED] readily accessible to MLO members through electronic communications accounts and by following standard MLO transaction procedures. As described above, UCC-1 boasted that the MLO operates in forty (40) countries. **KULIZHNIKOV** and [REDACTED] have each

explained in detail how they rely upon and coordinate with each other and the MLO's network to rapidly and efficiently service money laundering contracts around the world.

72. **KULIZHNIKOV** and [REDACTED] have each also exhibited clear knowledge that at least portions of the funds laundered by the MLO and the JUST Team are derived from drug trafficking. Agents have identified at least three drug traffickers directly serviced by **KULIZHNIKOV** (RASSOKHIN; the New York-based Oxycontin distributor; and UCC-3), in addition to the purported drug proceeds he agreed to launder on behalf of CS8, CS9, and CS10 during the undercover operations. Similarly, [REDACTED] has opined on how "reputation is important" in "this kind of business" with "drug dealers" and readily agreed to launder purported cocaine proceeds on behalf of CS8. UCC-1 has also openly engaged in drug-related conversation during money laundering negotiations. For example, during a February 2021 text conversation over SkyECC,¹³ an associate offered UCC-1 a series of money laundering contracts in various countries (including €120,000 in the Netherlands and the equivalent of €100,000 in Brazilian real in Sao Paolo, Brazil). In between the Dutch and Brazilian contract offers, the associate sent UCC-1 a photograph that appears to depict approximately forty (40) kilograms of cocaine, packaged in bricks bearing labels depicting the Russian flag and text, "RUSIA" (see below):

¹³ SkyECC was an encrypted messaging platform installed on modified cellphones. In 2021, French law enforcement authorities lawfully seized SkyECC servers and content, including communications with a PIN number identified as used by UCC-1. In or around October 2025, a certified copy of the communications seized from UCC-1's account was provided by France pursuant to a Mutual Legal Assistance Treaty request.



73. This partnership between the money launderers (**KULIZHNIKOV**, [REDACTED] [REDACTED] and others) exponentially enhances their individual profits and the MLO's overall operating capacity – since they are able to fulfill more money laundering contracts for their drug trafficking clients by leveraging the collective MLO's courier network in locations where they may not have their own direct contacts.

74. Based on the facts outlined above, I respectfully submit that there is probable cause to believe that from in or about at least May 2024, and continuing thereafter up to and including the present, the exact dates being unknown, the defendants **KULIZHNIKOV** and [REDACTED] unlawfully, knowingly, and intentionally combined, conspired, confederated, and agreed with others, known and unknown, within the Eastern District of Virginia and elsewhere, to commit violations of 18 U.S.C. § 1956(h) (Money Laundering Conspiracy) with two objects: concealment, in violation of 18 U.S.C. § 1956(a)(1)(B)(i), and sting, in violation of 18 U.S.C. § (a)(3)(B).

75. I also respectfully submit that there is probable cause to believe that on or about June 13, 2024, and on or about July 16, 2024, that [REDACTED] unlawfully, knowingly, and intentionally combined, conspired, confederated, and agreed with others, known and unknown, within the Eastern District of Virginia and elsewhere, to commit violations of 18 U.S.C. §§ 371, 1960 (Conspiracy to Conduct an Unlicensed Money Transmitting Business).

76. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

Melissa Schneider
Melissa Schneider
Special Agent
Drug Enforcement Administration

Attested to in accordance with the requirements
of Fed. R. Crim. P. 4.1 via telephone on
October 14, 2026.

John Anderson
Digitally signed by John
Anderson
Date: 2026.10.14 11:47:34 -04'00'
The Honorable John F. Anderson
United States Magistrate Judge

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

United States of America

v.

PAVEL ALEKSEYEVICH KULIZHNIKOV,
a/k/a "Pavel Alekseevich Kulizhnikov,"
a/k/a "Pasha,"
a/k/a "Panprezident1"

Case No. 1:26-MJ-407

UNDER SEAL*Defendant*

ARREST WARRANT

To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay
(name of person to be arrested) PAVEL ALEKSEYEVICH KULIZHNIKOV, a/k/a "Pavel Alekseevich Kulizhnikov," "Pasha," "Panprezident1",
who is accused of an offense or violation based on the following document filed with the court:

☐ Indictment ☐ Superseding Indictment ☐ Information ☐ Superseding Information ☒ Complaint
☐ Probation Violation Petition ☐ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:

Money Laundering Conspiracy, in violation of 18 U.S.C. § 1956(h), with two objects: concealment, in violation of 18 U.S.C. § 1956(a)(1)(B)(i), and sting, in violation of 18 U.S.C. § (a)(3)(B).

John Anderson

Digitally signed by John
Anderson

Date: 2026.10.14 11:48:08 -04'00'

Date: 10/14/2026

Issuing officer's signature

City and state: Alexandria, Virginia

The Hon. John F. Anderson, U.S. Magistrate Judge

Printed name and title

Return

This warrant was received on (date) _____, and the person was arrested on (date) _____
at (city and state) _____.

Date: _____
Arresting officer's signature

Printed name and title

INFORMATION
COPY ONLY
NOTICE: BEFORE ARREST, VALIDATE
THROUGH NCIC. ORIGINAL
HELD BY U.S. MARSHAL.