EYC/DMP:AFM/JAM/SM/MAB
F. #2021R00874

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
- X

UNITED STATES OF AMERICA

- against -

ANATOLY LEGKODYMOV,
also known as "Anatolii Legkodymov,"
"Gandalf" and "Tolik,"

Defendant.

- X

AMENDED AFFIDAVIT AND COMPLAINT IN SUPPORT OF AN APPLICATION FOR AN ARREST WARRANT

(T. 18, U.S.C., §§ 1960(b)(1)(b), 1960(b)(1)(c), 2 and 3551 et seq.)

No. 23-M-17

EASTERN DISTRICT OF NEW YORK, SS:

RYAN ROGERS, being duly sworn, deposes and states that he is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such:

Conducting an Unlicensed Money Transmitting Business

In or about and between January 1, 2016 and December 2022, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant ANATOLY LEGKODYMOV, also known as "Anatolii Legkodymov," "Gandalf" and "Tolik," (hereinafter "LEGKODYMOV" or "the defendant") did knowingly conduct, control, manage, supervise, direct or own part of a money transmitting business, which (a) failed to comply with the money transmitting business registration requirements under Title 31, United States Code, Section 5330, and the regulations prescribed thereunder, and (b) otherwise involved the transmission of funds known to LEGKODYMOV to have been

derived from a criminal offense or intended to be used to promote or support unlawful activity.

(Title 18, United States Code, Sections 1960(b)(1)(B), 1960(b)(1)(C), 2 and 3551 et seq.)

The source of your deponent's information and the grounds for his belief are as follows:[1]

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since January 2021. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for cybercrime and financial crime. I have investigated and otherwise participated in numerous matters during the course of which I have conducted physical surveillance, interviewed witnesses, executed court-authorized search warrants, and used other investigative techniques to secure relevant information.

2. I am familiar with the facts and circumstances set forth below from my participation in the investigation, from my review of documents obtained pursuant to the investigation, and from reports of other law enforcement officers involved in the investigation. When I rely on statements made by others, such statements are set forth only in part and in substance unless otherwise indicated. In addition, many of the statements described herein are based on draft English translations of communications that were not

---

[1] Because the purpose of this complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware. Where statements cited in this complaint have been translated from another language to English, they are presented in sum and substance only.

originally made in English, and are subject to revision.

I. STATUTORY BACKGROUND

3. Title 18, United States Code, Section 1960 prescribes criminal penalties for anyone who "knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business."

4. The statute defines the term "unlicensed money transmitting business" to mean, as relevant here, a money transmitting business that affects interstate or foreign commerce in any manner or degree and that either "fails to comply with the money transmitting business registration requirements under section 5330 of title 31, United States Code, or regulations prescribed under such section," 18 U.S.C. § 1960(b)(1)(B), or "otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity," 18 U.S.C. § 1960(b)(1)(C).

5. The "regulations" referenced in 18 U.S.C. § 1960(b)(1)(B) define a "money services business" ("MSB") as "[a] person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in" one or more specific capacities—including as a "money transmitter." 31 C.F.R. § 1010.100(ff). The term "[m]oney transmitter," in turn, includes anyone who "accept[s] . . . currency, funds, or other value that substitutes for currency from one person and . . . transmit[s] . . . currency, funds, or other value that substitutes for currency to another location or person by any means," as well as "[a]ny other person engaged in the transfer of funds." 31 C.F.R. § 1010.100(ff)(5)(i)(A)-(B).

6. All MSBs are required to register with the Financial Crimes

Enforcement Network ("FinCEN"), a division of the U.S. Department of Treasury, unless specific exemptions apply. 31 C.F.R. § 1022.380(a)(1). In addition, MSBs are required to comply with certain aspects of the Bank Secrecy Act, such as filing reports of suspicious transactions, 31 U.S.C. § 5318(g); 31 C.F.R. § 1022.320(a); and implementing an effective anti-money-laundering ("AML") program, 31 C.F.R. § 1022.210. An effective anti-money-laundering program is described as "one that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities." 31 C.F.R. § 1022.210(a). Under the regulations, an anti-money-laundering program must, at a minimum, "[i]ncorporate policies, procedures, and internal controls reasonably designed to assure compliance" with an MSB's obligations to verify customer identification, file reports, creating and retain records, and respond to law enforcement requests. 31 C.F.R. § 1022.210(d)(1). The obligation to verify customer identification is frequently referred to as a "know your customer," or "KYC," requirement.

7. In 2013, FinCEN issued guidance stating that the definition of a money transmitter includes an individual who offers exchange services between virtual currency and fiat currency. *See* Dep't of the Treasury FinCEN Guidance, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013) (the "FinCEN Guidance"). The FinCEN Guidance stated, among other things, that those who are money transmitters because they offer exchange services between virtual currency and fiat currency also come within the regulations applicable to MSBs. That guidance was reaffirmed in May 2019. Dep't of the Treasury FinCEN Guidance, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019).

II. BACKGROUND REGARDING THE DEFENDANT AND BITZLATO

8. Bitzlato Limited ("Bitzlato") is a Hong Kong-registered cryptocurrency exchange, founded in 2016, that operates globally. Bitzlato's customers can use the platform to purchase cryptocurrencies with cash, exchange cryptocurrencies for other cryptocurrencies, and send cryptocurrency to other users' wallets,[2] whether hosted by Bitzlato or external to the service. According to data publicly available on the blockchain, Bitzlato has processed approximately $4.58 billion worth of cryptocurrency transactions since May 3, 2018. A substantial portion of those transactions constitute the proceeds of crime, as well as funds intended for use in criminal transactions.

9. The defendant ANATOLY LEGKODYMOV ("LEGKODYMOV") is a 40-year-old Russian national who resides in Shenzhen, People's Republic of China. LEGOKDYMOV is a co-founder and senior executive of Bitzlato and is the company's majority shareholder. According to a copy of Bitzlato's organizational chart dated March 2021, LEGKODYMOV shares control over the company with his co-founder, an individual whose identity is known to me ("Executive-1"), who is Bitzlato's second-largest shareholder. Bitzlato's CEO reports directly to LEGKODYMOV and Executive-1.

---

[2] The storage of virtual currency is typically associated with an individual "wallet," which is similar to a virtual account. Wallets are used to store and transact in virtual currency. A wallet may include many virtual currency addresses, roughly equivalent to anonymous account numbers.

III. BITZLATO'S INADEQUATE KYC AND USAGE FOR ILLICIT TRANSACTIONS

10. As set forth below, the government's investigation has revealed that Bitzlato failed to establish an effective AML program. For most of Bitzlato's corporate history, it was a staple of the company's branding and online messaging that Bitzlato had loose or non-existent requirements as to "KYC." As an example, Bitzlato's website advertised for years (and as recently as March 31, 2022) that the site offered "Simple Registration without KYC. Neither selfies nor passports required. Only your email needed." Similarly, a blog post on Bitzlato's website stated: "On Bitzlato no KYC is required for you to trade." Beginning on or about February 28, 2022, Bitzlato began requiring new users to self-verify, but indicated in communications to users about the policy that verification for existing users was "not obligatory."

11. Bitzlato's failure to establish an effective AML program has facilitated its use by criminals laundering the proceeds of crime. Most prominently, Bitzlato had a reciprocal relationship with Hydra Marketplace ("Hydra"), an anonymous, illicit online bazaar (known as a "darknet market") that facilitated the sale of illegal drugs, stolen financial information, fraudulent identification documents, and money laundering services, including cryptocurrency mixing.[3] Hydra operated from approximately 2015 to April 5, 2022, when it was shut down by U.S. and German law enforcement. During that time, it grew to be

[3] Hydra functioned like well-known legitimate online marketplaces, such as eBay, by connecting buyers and sellers and facilitating transactions with an escrow service. Hydra facilitated payments by accepting virtual currencies from buyers in exchange for goods provided by vendors.

notorious as the largest and longest-running darknet market in the world. In 2021, Hydra accounted for 80% of darknet market revenue worldwide, and from January 2016 to March 2022, it received the equivalent of approximately $5.2 billion in cryptocurrency.

12. A substantial portion of the cryptocurrency that Hydra received was sent directly from wallets at Bitzlato. Hydra was Bitzlato's largest counterparty for cryptocurrency transactions, and Bitzlato served as Hydra's second-largest counterparty. Hydra buyers routinely funded their illicit purchases from cryptocurrency accounts hosted at Bitzlato, and in turn, sellers of illicit goods and services on the Hydra site routinely sent their illicit proceeds to accounts at Bitzlato.

13. The FBI has determined through blockchain analysis that users of Hydra sent approximately $170.6 million in cryptocurrency to wallets on Bitzlato between May 2018 and April 2022. In addition, during that same period, users of Hydra sent an additional $218.7 million to non-Bitzlato addresses from which they were then sent to Bitzlato.

14. The amount of money flowing from Bitzlato to Hydra was equally substantial between May 2018 and April 2022. Criminals who purchased goods and services on Hydra drew the equivalent of $124.4 million from Bitzlato accounts to make purchases on Hydra, and drew an additional $191.9 million from non-Bitzlato sources that had, in turn, been funded from Bitzlato.

15. In addition to funds exchanged with Hydra, Bitzlato has received, directly or indirectly, more than 15 million dollars' worth of cryptocurrency representing the proceeds of ransomware attacks, based on blockchain analysis by the FBI and the FBI's own information about the addresses to which ransoms have been paid. FBI agents have

informed me that, in the context of ransomware investigations, they have observed millions of dollars' worth of known ransom proceeds transferred to Bitzlato at the direction of ransomware actors, after which the funds are converted to cash.

16. Bitzlato's hospitability to criminal proceeds is a direct result of its deficient KYC policies, as exemplified by a recent discussion on a cybercriminal forum. On or about August 2, 2022, a confidential human source of the FBI ("CHS-1") reviewed postings on a Russian-language dark web cybercrime forum ("Forum A") used for criminal purposes. CHS-1 reported that on or about December 26, 2021, a user posted on Forum A, stating that he resided in "a prosperous capital in Asia" and had become acquainted with people who had large bitcoin holdings. The user asked for advice about stealing and laundering cryptocurrency from these acquaintances. Another user responded, warning the original poster against using Western, compliant cryptocurrency exchanges to launder the stolen funds, because they might trace and report the stolen funds: "Regarding the theft of coins . . . [d]on't try to immediately drag them to a KYC exchange, it's better to [send them to] a mixer or to our CIS[4] exchangers (like Bitzlato), they are unlikely to give you away to some clowns from the ass of Asia."

17. Forum A, and other locations on the internet, also contains numerous offers to sell or purchase straw-man accounts at Bitzlato, verified with identifying information from persons other than the accounts' true users, that could then be used by a different person to trade with effective anonymity. (The "straw man" registrant is

---

[4] "CIS" refers to the Commonwealth of Independent States, a group of countries roughly covering the territory of the former Soviet Union.

sometimes referred to in Russian slang as the "drop.") For example, there is a publicly accessible forum on Russian-language social networking site VK for people to discuss "Purchase/sale of bc [Bitcoin] drop accounts." A post within that forum, published on October 6, 2021, reads: "Need one person on Bitzlato with an [identity] document from the Russian federation, payment of 1000 rubles."[5]

18. I have learned from other FBI agents that, while Bitzlato provides the user data that it has collected in response to government requests, that data is often limited to minimal details, such as customers' usernames on Telegram, a secure messaging app.

19. Bitzlato's employees and managers knew that Bitzlato had deficient KYC procedures, and understood that these insufficient controls facilitated their customers' use of Bitzlato to transmit illicit proceeds and funds destined to be spent on criminal activity.

20. For instance, Bitzlato's customer-service chat portal has received a steady stream of questions from Bitzlato users about transacting with Hydra, and money laundering more generally. Although Bitzlato sometimes blocked or terminated users who had transacted with Hydra or were otherwise suspected of engaging in drug transactions, its employees sometimes helped users to carry out transactions with Hydra, and sometimes took no action either way.

21. Overall, Hydra was mentioned hundreds of times in customers' communications with Bitzlato. Some examples include the following:

---

[5] Available at https://vk.com/wall-104537593_56487 (last accessed December 12, 2022)

- On or about December 27, 2017, a user with the username "Dude Weed" wrote to Bitzlato's customer service portal, stating: "I have a bitcoin wallet in my account on the Hydra site. I also have a wallet here . . . How do I recharge a Hydra wallet"? The user also provided transaction details. Based on my training and experience, this query reflects the user's desire to send funds from Bitzlato to Hydra. A Bitzlato representative responded: "Hello dude weed," apologized for the delay in the transaction, and stated that "The transaction successfully went online." The Bitzlato representative provided a link to an online blockchain explorer, reflecting a completed Bitcoin transaction whose total amount was then equivalent to approximately $14,600.
- Similarly, on or about March 5, 2020, a Bitzlato user wrote to the customer service portal: "I buy opiates in Hydra . . .but I did not get the address." A Bitzlato employee responded: "Thank you for contacting us! Please provide the transaction number."
- On or about October 18, 2020, a Bitzlato user wrote to the portal, asking if he could transfer funds "from this wallet to hydra." A Bitzlato representative responded: "You can transfer BTC[6] to any actual address. There are no restrictions for any individual services."
- On or about May 5, 2021, a user asked whether he could "exchange dirty bitcoin for Sber without problems here"—an apparent reference to Sberbank, a Russian bank. A Bitzlato representative asked the user to clarify, and he wrote: "Well for example the person sent me to my wallet bitcoins taken from darknet, some kind of illegal exchanges, as far as I know they automatically get to dirty bitcoins. So my question is, when I transfer them to Sberbank in rubles, can I change them?" The Bitzlato representative responded that "In this case there are no limitations from the service in this matter."

---

[6] "BTC" is the standard abbreviation for bitcoin.

- On or about August 18, 2021, a user complained that he or she had "had my account stolen when I was transferring btc to hydra. What should I do? Is there any way to get bitcoins back from the wallet?" A Bitzlato representative asked, "What can we do for you?" and, after further exchanges, stated that "[a]ll bitcoin transactions are irreversible."
- On or about March 31, 2020, a user wrote that he wanted to use a "free withdrawal voucher" provided by Bitzlato and asked if the voucher could be used to transfer funds to Hydra, commenting that he did not want to withdraw to "third party wallets." The customer service representative replied in the affirmative but corrected the user, noting that "Hydra is a third party service."
- On or about March 26, 2022—mere days before Hydra was seized—a customer wrote that he wanted 'top up my wallet on Hydra . . . I want to replenish my wallet on Hydra." He received instructions on how to do so.

22. Bitzlato's customer service representatives also received communications demonstrating that customers were using accounts that had been opened with others' credentials and carrying out straw-man transactions on behalf of others. Based on my training and experience, individuals regularly use straw-man accounts to obfuscate their true identity when using funds from illicit sources or illicit purposes. Bitzlato did not consistently terminate or penalize such customers and, in fact, had a practice of accepting straw-man credentials as verification for accounts. As examples:

- On December 17, 2020, a Bitzlato representative asked a user to provide his identity documents. The user protested, writing, "I don't quite understand why you need a photo of this card? It's not mine[.]" In further conversations, the user clarified that "everyone on the site trades with other people's cards . . . they often discuss so-called 'drops.'" The user commented that he had been told to create an account using credentials supplied by an online cryptocurrency training course that he had found on Instagram. The Bitzlato representative asked the user to provide his true

identity documents and, rather than terminate that user, said the user could keep trading on Bitzlato.

- On or about May 7, 2022, a Bitzlato user was asked to provide his identifying information. The user responded that he was "not going to lie to you and tell you tales[.] I bought this account—bought it, I'm telling you." The user added that there were "hundreds of these accounts with passed verifications—as if you didn't know that." The user offered to "find the man" whose credentials had been used to verify the account, and "pay him to send everything you need, because the money is mine." The Bitzlato representative responded: "That's your right."
- On or about August 28, 2022, a Bitzlato representative told a user that his account was blocked because he had been transacting with wallets that were "linked to criminal activity." The user responded that he had been only "the middleman for the transfer," explaining that his brother had "offered to give me the contact of his acquaintance, saying that he sometimes exchanges bitcoins and that I could work with him. He said there was nothing to worry about and that 'his bitcoin was clean.'" The user explained that he accepted cash from this acquaintance and used it to make cryptocurrency transactions on the person's behalf "without any questions (where and why)" and without ever having met the person. The Bitzlato representative unblocked the account but asked the user to stop engaging in such transactions.
- On or about September 12, 2022, Bitzlato blocked a user's account and asked him to verify his identity. The user responded that he would provide "a woman's" identity documents, adding: "Am I an idiot to verify myself? Verify the 'drop.'" The user added that he would be transferring ransomware proceeds and "a payment from Hydra" to his Bitzlato account. The Bitzlato customer service representative responded that an account verified in the name of the user's "drop," or straw man, would "belong to your drop," and concluded: "Okay, we are waiting for the application."

IV. THE DEFENDANT AND OTHER SENIOR MANAGERS WERE AWARE OF BITZLATO'S INADEQUATE KYC AND ILLICIT FUNDS

23. Bitzlato's senior managers, including LEGKODYMOV, were aware of the high volume of criminal funds, including narcotics-related funds, that were transacted on the site, due to their deliberate decision not to verify the true identities of its users.

24. Bitzlato personnel used an internal chat service to discuss their administration of the service. In one such chat, on or about October 4, 2018, Executive-1 reported to LEGKODYMOV that Bitzlato faced a "threatening situation" in the bitcoin market: "no small-time dealers, seems they've been scared off by the drug war." The result, he said, was that there were not enough users seeking to sell bitcoin cheaply on Bitzlato: "We've been advertising from 5,000 [rubles] to buy, but I guess junkies only buy for 1,000 to 3,000."

25. As a solution, Executive-1 advocated going easy on drug dealers: "[I]f we seriously announce the fight against drug traffickers, they will just be dumped on another platform. My suggestion is to fight them nominally, ie, block once a month when they can clearly be found." The current "zealous" approach to blocking drug-related users, Executive-1 said, would be "not very correct from a business point of view."

26. LEGKODYMOV responded by noting that the proceeds from drug dealers' seized cryptocurrency wallets was potentially "a bonus" to Bitzlato's coffers. He then recommended following "the policy of the banks" – "If you make a transfer 'for cannabis' then they will probably block you, of course, but no one will look for it that way."

27. On or about April 23, 2019, Executive-1 again warned his colleagues, including the defendant, that "bitzlato clients are addicts who buy drugs at the hydra site and

similar resources." LEGKODYMOV responded that Bitzlato could expand by offering anonymous financial services to run-of-the-mill individuals, such as taxi drivers. LEGKODYMOV stated that "[e]veryone wants to keep their [identity] cards out of sight."

28. LEGKODYMOV was also aware that Bitzlato's customers were not using the service under their true identities. On or about May 29, 2019 LEGKODYMOV wrote to a colleague in a chat: "All traders are known to be crooks. Trading on 'drops,' etc. You do realize that they all (I think 90%) do not trade on their [identity] cards." "Yes," the colleague responded.

29. Later that year, on or about June 22, 2019, LEGKODYMOV commented: "Scammers know that it is possible to be verified for a drop and 100% withdraw money." Based on my training and experience, I understand this to indicate that the defendant was aware that Bitzlato's procedures to verify customers' identities were easily circumvented through the use of "drops," allowing users to withdraw illicit funds anonymously.

30. Bitzlato's inadequate verification procedures and transactions in criminally linked funds were summed up in a document titled "Competitor Analysis," drafted by Bitzlato's Marketing Director, that was saved to a shared cloud drive associated with Bitzlato's "management" email account. The document contained an analysis of the pros and cons of Bitzlato and its competitor sites. The document noted the following regarding Bitzlato:

Positives	Negatives
No KYC 3 interfaces Bitcoin checks Instant addition of new payment methods 9 coins traded	Dirty money Lots of scams High fees to withdraw

31. Based on my training and experience, this chart reflects its drafter's awareness that Bitzlato had ineffective KYC procedures and handled a significant volume of illicit funds.

V. BITZLATO DOES BUSINESS IN SUBSTANTIAL PART IN THE UNITED STATES, INCLUDING IN THE EASTERN DISTRICT OF NEW YORK

32. Although Bitzlato is headquartered outside the United States, it conducts business in substantial part in the United States. Among other things, the evidence collected to date establishes that despite public claims to the contrary, Bitzlato knowingly serviced U.S. customers; conducted transactions with U.S.-based exchanges; and was run using U.S. online infrastructure—and, for at least some period of time, was being managed by the defendant while he was in the United States.

33. Bitzlato has, at times, claimed that it does not allow U.S.-based individuals to use its platforms. But that rule is not consistently enforced. To the contrary, on or about December 13, 2022, CHS-1, who used non-U.S. identity documents for the purpose, was able to sign up for a Bitzlato account from a U.S. IP address located in New York City. Moreover, Bitzlato's customer service representatives have repeatedly advised users that they were permitted to transact with the United States. On or about December 16, 2020, for example, a user asked whether he could "use American bank cards to buy and sell [cryptocurrency]." A Bitzlato representative replied: "Yes, of course. Choose USD

currency in 'Preferences.'" Similarly, on January 20, 2021, a Bitzlato user asked whether he could "get money from the U.S. to this wallet." A Bitzlato representative replied: "You can transfer funds from anywhere in the world."

34. In addition, Bitzlato executives, including LEGKODYMOV, were aware based on internal data that Bitzlato had a significant U.S. user base. For example, LEGKODYMOV received periodic emails from a U.S. provider of cybersecurity services that controlled and filtered access to Bitzlato's website. Those emails reflected substantial traffic to the website from U.S.-based Internet Protocol addresses.[7] Most recently, on August 9, 2022, LEGKODYMOV received an email reflecting that in July, Bitzlato's website had received approximately 264 million visits from U.S.-based IP addresses, making the United States the fourth most common source of internet traffic for Bitzlato.

35. Moreover, in response to requests for account data from U.S. law enforcement agents about specific users who were the subjects of law enforcement investigations, Bitzlato personnel provided charts that reflected the Internet Protocol addresses from which those users were logging into Bitzlato's servers. Those charts included a column titled "user_ip_country," reflecting the country in which each IP address appeared to be located. In numerous instances, the Bitzlato charts reflected that users were accessing Bitzlato's servers from the United States, including logins from an IP address located in Brooklyn, New York that was identified in October 2022.

---

[7] An Internet Protocol, or "IP," address is a unique numerical string denoting a particular access point to the internet. Through the use of commercial and open-source databases, it is generally possible to geolocate an IP address by country.

36. I have reviewed information provided by a U.S.-based cryptocurrency exchange ("Exchange-1"). Exchange-1 has indicated that since May 24, 2018, more than 1,600 of Exchange-1's U.S.-based customers—including 174 customers located in the Eastern District of New York—have sent money from their wallets at Exchange-1 to wallets hosted by Bitzlato, for a total volume of approximately $2.4 million.

37. In addition, Bitzlato made use of U.S. vendors for core aspects of its service, including Bitzlato's corporate email, its customer service platform, and the cybersecurity vendor described above.

38. In or around October 2022, LEGKODYMOV arrived in the United States at John F. Kennedy Airport in Queens, New York. LEGKODYMOV is presently in or around Miami, Florida. LEGKODYMOV has continued to administer Bitzlato while in the United States; data provided by the internet service provider at the location in Florida where he is residing indicates that LEGKODYMOV connected hundreds of times to Bitzlato's management server between December 24, 2022 and January 2, 2023.

39. LEGKODYMOV was interviewed when seeking admission into the United States by a U.S. Customs and Border Protection ("CBP") officer, who asked him about his employment. LEGKODYMOV did not disclose his connection to Bitzlato. However, the CBP officer conducted a border search of LEGKODYMOV'S mobile devices and found that they contained numerous recent communications related to Bitzlato, including a recent chat titled in part "bitzlato.com admin chat," and a second recent chat titled "Bitzlato Support Chat."

WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendant ANATOLY LEGKODYMOV, also known as "Anatolii

Legkodymov," "Gandalf" and "Tolik," so that he may be dealt with according to law.

IT IS FURTHER REQUESTED that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including this Affidavit and the arrest warrant for the defendant ANATOLY LEGKODYMOV. Based on my training and experience, I have learned that criminals actively search for criminal affidavits on the Internet and disseminate them to other criminals as they deem appropriate, such as by posting them publicly through online forums. Premature disclosure of the contents of this Affidavit and related documents will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior and notify confederates.

RYAN ROGERS
Special Agent
Federal Bureau of Investigation

telephonically

Sworn to before me this
14th day of January, 2023

Robert Levy

THE HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK