

# UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

Alhasan altonuk Eltoky

Defendant

Case No. 2:20-Mj-02993

## CRIMINAL COMPLAINT BY ELECTRONIC MEANS .

I, the complainant in this case, state that the following is true to the best of my knowledge and belief. Beginning no later than May 05, 2020 and continuing through at least July 17, 2023, in the county of Los Angeles, in the Central District of California, and elsewhere, the defendant conspired to hack and launder proceeds fraudulently hijacked from a forex & crypto investment firm, a foreign financial firm and an English premier league club in violation of:

*Code Section*

18 U.S.C. § 1956(h)

*Offense Description*

Conspiracy to Engage in Money Laundering

This criminal complaint is based on these facts:

*Please see attached affidavit.*

Continued on the attached sheet.

*Complainant's signature*

Derrick Graham special agent FBI

*Printed name and title*

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

Date: Date 06/25/2024

*Judge's signature*

City and state: Los Angeles, California

Hon. Rozella A. Oliver, U.S. Magistrate Judge

*Printed name and title*

## **AFFIDAVIT**

I, DERRIK GRAHAM, being duly sworn, declare and state as follows:

### **I. INTRODUCTION**

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and have been so employed since approximately March 2015. I am currently assigned to the Los Angeles Field Office, High-Tech Organized Crime Squad, where I primarily investigate cyber-enabled fraud and business email compromise (“BEC”) schemes. Between approximately August 2015 and December 2018, I was assigned to a cyber-crime squad in the Chicago Field Office, where I investigated cyber-related crimes, including BEC cases. During my career as an FBI Special Agent, I have participated in numerous computer crime investigations. In addition, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations, computer technology, and white-collar fraud.

2. This affidavit is made in support of a criminal complaint against, and arrest warrant for, Alhasan Altonuk (“Eltoky”), for violation of 18 U.S.C. § 1956(h) (Conspiracy to Engage in hacking cryptocurrencies & Money Laundering).

3. The facts set forth in this affidavit are based upon my personal involvement in this investigation, my review of reports and other documents related to this investigation, my training and experience, and information obtained from other agents, law enforcement officers, and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and arrest warrant, and does not purport to set forth all of my knowledge of the government’s investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. Unless specifically indicated otherwise, all dates set.

## II. SUMMARY OF PROBABLE CAUSE

4. Alhasan Altonuk (“Eltoky”) participated in these fraudulent schemes and money laundering in coordination with multiple coconspirators, including the persons referred to herein as Coconspirator 1 and Coconspirator 2.

5. This affidavit discusses several fraudulent schemes involving ALHASAN. First, messages found on the iPhone of Coconspirator 1 (reviewed pursuant to a federal search warrant issued in this District) reflect that ALHASAN, Coconspirator 1, and Coconspirator 2, with others, hacked the vault of a forex and cryptocurrency investment firm

which ALHASAN worked for at their branch in Delaware United States of approximately \$21,922,857.76, including approximately \$3,596,050 in cryptocurrency that Alhasan, Coconspirator 1, and Coconspirator 2 laundered while Coconspirator 2 was in Delaware, united states.

6. Second, ALHASAN and Coconspirator 1 conspired to launder funds intended to be stolen through fraudulent wire transfers from a foreign financial institution (the “Foreign Financial Institution”), in which fraudulent wire transfers, totaling approximately €13 million (approximately USD \$14.7 million), were sent to bank accounts around the world in February 2019. Coconspirator 1 conspired with the hacker who initiated the fraudulent wire transfers, and also conspired with a number of others, including ALHASAN, to launder the funds that were intended to be stolen. ALHASAN, specifically, provided Coconspirator 1 with two bank accounts in Europe that ALHASAN anticipated would each receive €5 million of the fraudulently obtained funds. Other communications between ALHASAN and Coconspirator 1 indicate that, in addition to these schemes, ALHASAN and Coconspirator 1 conspired to launder tens, and at times hundreds, of millions of dollars that were proceeds of other fraudulent schemes and computer intrusions, including a fraudulent scheme to steal 100 million pounds from an English Premier League football club.

## II. SUMMARY OF PROBABLE CAUSE

4. Alhasan Altonuk (“Eltoky”) participated in these fraudulent schemes and money laundering in coordination with multiple coconspirators, including the persons referred to herein as Coconspirator 1 and Coconspirator 2.

5. This affidavit discusses several fraudulent schemes involving ALHASAN. First, messages found on the iPhone of Coconspirator 1 (reviewed pursuant to a federal search warrant issued in this District) reflect that ALHASAN, Coconspirator 1, and Coconspirator 2, with others, hacked the vault of a forex and cryptocurrency investment firm

which ALHASAN worked for at their branch in Delaware United States of approximately \$21,922,857.76, including approximately \$3,596,050 in cryptocurrency that Alhasan, Coconspirator 1, and Coconspirator 2 laundered while Coconspirator 2 was in Delaware, united states.

6. Second, ALHASAN and Coconspirator 1 conspired to launder funds intended to be stolen through fraudulent wire transfers from a foreign financial institution (the “Foreign Financial Institution”), in which fraudulent wire transfers, totaling approximately €13 million (approximately USD \$14.7 million), were sent to bank accounts around the world in February 2019. Coconspirator 1 conspired with the hacker who initiated the fraudulent wire transfers, and also conspired with a number of others, including ALHASAN, to launder the funds that were intended to be stolen. ALHASAN, specifically, provided Coconspirator 1 with two bank accounts in Europe that ALHASAN anticipated would each receive €5 million of the fraudulently obtained funds. Other communications between ALHASAN and Coconspirator 1 indicate that, in addition to these schemes, ALHASAN and Coconspirator 1 conspired to launder tens, and at times hundreds, of millions of dollars that were proceeds of other fraudulent schemes and computer intrusions, including a fraudulent scheme to steal 100 million pounds from an English Premier League football club.

## STATEMENT OF PROBABLE CAUSE

### A. Identification of ALHASAN

7. Analysis of Coconspirator 1's iPhone and other online accounts showed that Coconspirator 1 operated and tasked money mule crews for a number of fraudulent schemes, including BEC schemes and cyber-heists. Analysis also showed that Coconspirator 1 communicated with the U.A.E. phone number +971543777711 ("Phone Number 1"), phone number +18435855307 and +12136612342 about multiple fraudulent schemes and money laundering. As described below, Phone Number 1 was one of the phone numbers ALHASAN used during 2019 and 2020.

8. Information from his email and social media accounts, financial records, and internet research, some of which is further discussed below.) Records from Apple Inc. showed the following:

- a. The email account [alhasanaltonuk@gmail.com](mailto:alhasanaltonuk@gmail.com) was used to create an Apple account on March 29, 2014, which was active as of June 2024, and used the subscriber's name "ELTOKY."

Based on my review and an FBI computer scientist's review of Google account records for [alhasanaltonuk@gmail.com](mailto:alhasanaltonuk@gmail.com), obtained through legal process and a federal search warrant in this District, I know the following:

- a. The account used the subscriber name "ELTOKY" and was created on September 19, 2013. Additionally, the recovery email listed was [eltoky@icloud.com](mailto:eltoky@icloud.com), and the recovery phone number was Phone Number 2.
- b. Multiple emails in the email account [eltoky@gmail.com](mailto:eltoky@gmail.com) confirmed that ALHASAN used Phone Number 1, Phone Number 2, and Phone Number 3.
- c. The email account [alhasanaltonuk@gmail.com](mailto:alhasanaltonuk@gmail.com) also contained emails with attachments relating to wire transfers in large dollar values, including wire transfers in February 2018 in the amounts of \$250,000 and \$2,397,000.

Based on the context of the emails, as well as other information gathered during the FBI investigation about one of the sender email accounts, it appears that these emails were related to fraudulent transactions.

9. Other financial records corroborate ALHASANS' identity.

a. Records from Western Union indicate that two money transfers—one listing Phone Number 1 and one listing Phone Number 3 occurred in UAE in 2018, in which the sender was listed as ALHASAN, with a birthdate of October 11, 1977, and using an identification bearing the same phone number.

10. Other evidence corroborates that ALHASANS' birthdate is October 11, 1977, and that he is "Eltoky."

a. A United States immigrant visa application submitted in December 2011 listed ALHASANS' full name and his birthdate as October 11, 1982.

b. Moreover, I reviewed information publicly viewable on the profile of the above-referenced "Eltokys" Instagram account that is consistent with ALHASANS' birthdate being on or about October 11. Specifically, on October 12, 2018, the account posted an image of a birthday cake with the inscription "Happy Birthday" and included the caption "Thank you all so much for the love you showed me yesterday till now."

### **The Victim Forex and Cryptocurrency investment firm**

In reviewing data from Coconspirator 1's iPhone, I and another FBI employee saw messages reflecting that, in or around June 2020, ALHASAN had conspired with Coconspirator 1 and Coconspirator 2 to commit a fraudulent wire transfer and money-laundering scheme, in which a U.S. victim (the "Foreign Financial Institution") lost approximately \$21,922,857.76, including approximately \$3,596,050 all in crypto currencies. The messages reflected that part of the scheme, including acts in furtherance of the conspiracy, occurred while Coconspirator 2 was physically present in the United States.

### **C. The Foreign Financial Institution**

11. Based on information from FBI agents investigating the cyber-heist from the Foreign Financial Institution, I know that, on February 12, 2019, the Foreign Financial Institution suffered a computer intrusion and cyber-heist in which approximately €13 million (approximately \$14.7 million) was fraudulently wired from the Foreign Financial Institution to bank accounts in multiple countries.

12. Coconspirator 1 and ALHASAN, who used Phone Number 1 in these communications, exchanged messages discussing the cyber-heist from the Foreign Financial Institution. Based on my review of data from Coconspirator 1's iPhone and his Online Account, and discussions with FBI special agents and other law enforcement personnel familiar with this investigation, I know the following:

a. In a message on January 16, 2019, Coconspirator 1 contacted ALHASAN asking for two European bank accounts that could receive "5m euro" (€ 5million), which he said would be from the country in which the Foreign Financial Institution is located (the "Foreign Financial Institution Country"). Coconspirator1 stated several times that the "hit" would occur on February 12.

b. After some discussion, ALHASAN sent Coconspirator 1 the account information for a Romanian bank account, which he said could be used for "Large amounts."

c. ALHASAN further said he could provide another account, and Coconspirator 1 said that it would be a payment of "5m"—i.e., € 5 million—to each account.

d. On February 1, 2019, Coconspirator 1 told ALHASAN that a coconspirator said that "12th February they doing it[.] I have 4 spots Available[.] u gave me 1/4[.] try to get me a next one pls it will both done at once." Coconspirator 1 also sent ALHASAN a photograph of a computer screen containing a messaging conversation which discussed a February 12 "drop" and a "cashout."

e. On February 7, 2019, Coconspirator 1 told ALHASAN, “12th feb they lunching [sic “launching”] the swift I need 1 more from you pls.” Coconspirator 1 later explained, “I have 6 slots in total [¶] All 5m Euro [¶] Big hit in 12th feb [¶] They will all credit same time.”

i. SWIFT, or the Society for Worldwide Interbank

Financial Telecommunication, provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized, and reliable environment. SWIFT also sells software and services to financial institutions, much of it for use on the SWIFTNet network. SWIFT does not facilitate funds transfers. Rather, it sends payment orders, which must be settled by correspondent accounts that the institutions have with each other. Each financial institution, to exchange banking transactions, must have a banking relationship by either being a bank or affiliating itself with one (or more) bank(s) so as to enjoy those particular business features.

ii. I further know, based on my experience with this investigation, and from FBI agents investigating Coconspirator 1 and other targets, that hackers sometimes will attempt to conduct cyber-heists by gaining access to a bank’s computer network and then sending fraudulent and unauthorized SWIFT messages.

f. On February 10, 2019, Coconspirator 1 told ALHASAN, “Brother tonight is my dead line to submit anything more,” and then asked, “Do u want add one more or just stick to that one u gave me?” The next day, ALHASAN responded, and provided account information for another bank account in Bulgaria.



g. A photograph, dated February 13, 2019, found in Coconspirator 1's Online Account showed a computer screen with a messaging conversation in which Coconspirator 1 and another person discussed a number of "drops," i.e., bank accounts that could receive fraudulent funds. One participant said that there could only be "1 euro" drop, and they then discussed how many of Coconspirator 1's drops would be used. The username known to be used by Coconspirator 1 stated, "I have 3 euro 1 use [redacted] 2 Romania 1 Bulgaria 1 use."

h. On February 12, 2019, Coconspirator 1 told ALHASAN, "Wire is completed . . . We did it [redacted] 500k euro n [redacted] Should be on ur side by now."

i. In the conversation that followed, Coconspirator 1 told ALHASAN that there was only one wire to the account in Romania, "Sender name: tipico group limited [redacted] Country: [Foreign Financial Institution Country] [redacted] Amount: 500k euro. . . It's there now my other crew confirmed it's there as well[.]" Later, while they were trying to figure out whether the wire had been successful, Coconspirator 1 added, "They did me 3 wires (2 to euro 1 to USA) . . . Bank it came from is: [Foreign Financial Institution] . . . Brother, we still have access and they didn't realize, we gonna shoot again tomoro am." ALHASAN then confirmed that Coconspirator 1 was saying that the new wire would be sent to the second bank account he provided to Coconspirator 1, in Romania.

j. An image of a conversation saved in Coconspirator 1's Online Account, dated February 12, 2019, with a person other than ALHASAN, discussed a payment specifically from the Foreign Financial Institution. The conversation in the image stated, "my guy also deleted history logs at the bank so they won't even c the transaction."

k. The next day, February 13, 2019, after ALHASAN sent screenshots showing that the funds had not arrived in the Romanian bank account, Coconspirator 1 responded, “Today they noticed and pressed a recall on it, it might show and block or never show.” Coconspirator 1 then sent an image of a news article to ALHASAN detailing the theft of funds from the Foreign Financial Institution, followed by a message stating “Look it hit the news.” ALHASAN then replied “damn.”

l. Coconspirator 1 then wrote to ALHASAN: “Next one is in few weeks will let U know when it’s ready. too bad they caught on or it would been a nice payout.

### **Additional Fraudulent Schemes and Attempted Money Laundering**

14. In addition to participation in those fraudulent schemes, ALHASAN and Coconspirator 1 discussed additional BEC frauds and/or other fraudulent schemes in 2019. These included schemes where ALHASAN and Coconspirator 1 sought to fraudulently obtain millions—and, at times, hundreds of millions—of U.S. dollars and U.K. pounds sterling, as described below.

15. On March 10, 2019, Coconspirator 1 requested a bank account in the U.A.E. from ALHASAN into which approximately \$5 million could be deposited from a victim in the United States. Coconspirator 1 told ALHASAN that the “job” would be “Monday am USA time,” and, after some discussion, wrote, “Brother I need it now or we will lose our chance pls.” ALHASAN responded by providing bank account information for an account at Commercial Bank International in Dubai, U.A.E.

16. On April 30, 2019, Coconspirator 1 told ALHASAN, “Brother I have 4 company’s in uk ready to switch bank account on file but account has to be open beneficiary.” After some discussion, Coconspirator 1 further stated, “I have a room working for me, we have leads and company contracts . My guy is changing acc on file for 100m contracts and there payment are once or twice a week 1-5m [¶] I have 4 ready to switch up.”

a. Based on my training and experience, it appears Coconspirator 1 was referring to a BEC scheme, because BEC schemes often involve a hacker or fraudster tricking a victim into sending a payment to a coconspirator’s account by switching bank account information on payment instructions provided to the victim. I also know that an “open bene” or “open beneficiary” account is a bank account where a different business account name can be substituted to help in deceiving the victim into sending funds.

b. It thus appears that Coconspirator 1 was telling ALHASAN that coconspirators were fraudulently obtaining \$1 million to \$5 million through a BEC scheme once or twice a week, and was asking ALHASAN for a bank account that could be used to receive such funds.

17. On May 3, 2019, Coconspirator 1 told ALHASAN, “I need uk open beneficiary acc for Monday bro !!!!! [¶] Today I they paid me.” Coconspirator 1 also sent ALHASAN an image of a message from another person saying, “Yo [¶] 3 invoices totaling 1.1 M going into that account today . . . 346k 256k and 507k.” Coconspirator 1 then said, “Bro I have a room ready.” In the resulting discussion, Coconspirator 1 told ALHASAN that he was “doing invoice account swap” and needed “account open beneficiary.” When ALHASAN asked, “Which country,” Coconspirator 1 responded, “U tell me what country is best i attack [¶] But [¶] I have uk [¶] Ready live.”

16. On April 30, 2019, Coconspirator 1 told ALHASAN, “Brother I have 4 company’s in uk ready to switch bank account on file but account has to be open beneficiary.” After some discussion, Coconspirator 1 further stated, “I have a room working for me, we have leads and company contracts . My guy is changing acc on file for 100m contracts and there payment are once or twice a week 1-5m [¶] I have 4 ready to switch up.”

a. Based on my training and experience, it appears Coconspirator 1 was referring to a BEC scheme, because BEC schemes often involve a hacker or fraudster tricking a victim into sending a payment to a coconspirator’s account by switching bank account information on payment instructions provided to the victim. I also know that an “open bene” or “open beneficiary” account is a bank account where a different business account name can be substituted to help in deceiving the victim into sending funds.

b. It thus appears that Coconspirator 1 was telling ALHASAN that coconspirators were fraudulently obtaining \$1 million to \$5 million through a BEC scheme once or twice a week, and was asking ALHASAN for a bank account that could be used to receive such funds.

18. On May 7, 2019, Coconspirator 1 sent ALHASAN a photograph of an apparent banking website showing a transaction “due to be paid” of approximately 1,110,447 of some currency, which is around the same amount as the discussion described in the prior paragraph. Coconspirator 1 then wrote, “I sent 1.1m pound I have other companies ready to swap bro pls help me out I am losing millions.” ALHASAN then stated, “I will paste u one today,” and Coconspirator 1 responded,

“When we swap bro the only thing we change is iban or acc on file and we keep all other info as original but we can put acc name on the memo , u need acc that can handle millions and not block.” The next day, after Coconspirator 1 stated,

“Brother my guy can do refund to any visa debit card [¶] Just need card number exp and name,” ALHASAN and Coconspirator 1 had some additional discussion that appeared to be about credit card numbers, culminating with ALHASAN providing bank account information for an account in Mexico.

19. On May 12, 2019, Coconspirator 1 wrote to ALHASAN, “Brother tonight we are gonna swap ur acc on a big contract payment will be 3-6m every week [¶] I give u confirmation in 12he [¶] From uk.” After ALHASAN acknowledged the message, Coconspirator 1 wrote on May 13, 2019, “Your acc has been updated on file, give me 2hr I will send unall details my workers just went to sleep.” ALHASAN responded, “Waiting.”

20. Coconspirator 1 then sent messages to ALHASAN about the apparent victims. First, Coconspirator 1 sent the name of an English Premier League football club, listing the club’s address as the stadium where the club plays. Coconspirator 1 also wrote, “Amount 100M £,” indicating that the fraudulent transaction would be for 100 million. Second, Coconspirator 1 sent the name of a U.K. company with an address in Edinburgh, Scotland, and wrote, “Amount 200m £.” Coconspirator 1 then added, “We swapped ur acc under 2 contracts . Tomorrow morning we will send u the previous payment and amount with future paymanet and amount [¶] Can I have 1 more for tomorow to swap pls.”

21. In response, ALHASAN stated, “Bro [¶] I can’t keep collecting houses, not give them feedback, and keep asking for more. This thing costs a lot of money now to open.” ALHASAN and Coconspirator 1 then discussed the use of the account, and Coconspirator 1 sent a photograph of a computer screen showing the Mexican bank account information with the name of a U.K. company, with a U.K. address, substituted as the beneficiary information. ALHASAN responded, “When it’s done, let me know.”

a. I know based on my training and experience, and from other FBI agents who have experience with these matters, that Nigerian-origin subjects sometimes use the words “aza” (sometimes “azar,” “azza,” or “azah”) or “house” to refer to a bank account used to receive proceeds of a fraudulent scheme. The word “house” is also sometimes used to refer to a bank itself. I observed that, in other messages with ALHASAN, Coconspirator 1 used the term “azza,” in addition to using the term “house.” (While Coconspirator 1 is not Nigerian, he is known to have communicated with multiple Nigerian-origin coconspirators.)

22. On July 3, 2019, Coconspirator 1 reported to ALHASAN, “Brother I can’t send from uk to Mexico they keep finding out, but uk 2 uk these guy keep paying and I can show u my last week cashout.” He also added that another coconspirator “has acces to a European bank and want to initiate a MT103/202 10-50 million if u know about it.”

a. I know based on my training and experience that MT103 and MT202 are types of SWIFT messages. It thus appears that Coconspirator 1 was referencing a cyber-heist scheme in which a coconspirator would be able to make fraudulent transfers of 10 million to 50 million in dollars or euros

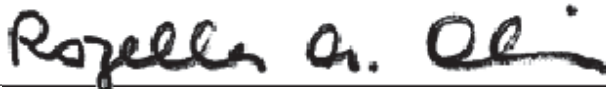
## CONCLUSION

23. For all the reasons described above, there is probable cause to believe that ALHASAN has committed a violation of 18 U.S.C. § 1956(h) (Conspiracy to Engage in Money Laundering).

---

DERRIK GRAHAM  
Special Agent  
Federal Bureau of Investigation

Attested to by the applicant in  
accordance with the requirements of  
Fed. R. Crim. P. 4.1 by telephone on  
June 25, 2020.



---

THE HONORABLE ROZELLA A. OLIVER  
UNITED STATES MAGISTRATE JUDGE