

**IN THE UNITED STATES DISTRICT COURT FOR THE
FOR THE DISTRICT OF COLUMBIA**

UNITED STATES OF AMERICA

V.

MEHMET AKTI & HÜSAMETTIN KARATAŞ

Case: 1:20-mj-00157
Assigned To : Harvey, G. Michael
Assign. Date : 8/12/2020
Description: Complaint w/ Arrest Warrant

**AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A
CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Special Agent Jonathan Gebhart, being duly sworn, depose and state as follows:

I. INTRODUCTION AND SUMMARY OF PROBABLE CAUSE

1. I seek a criminal complaint charging Mehmet Akti (“Akti”) and Hüsamettin Karataş (“Karataş”) with: (1) operating an unlicensed money transmitting business, in violation of Title 18, United States Code, Section 1960; and (2) conspiring to launder monetary instruments, in violation of Title 18, United States Code, Section 1956(h). Between in or about October 2017, and in or about August 2019, the defendants, Turkish nationals, accessed the U.S. financial system, and both knowingly operated an unlicensed money transmitting business and conspired to launder monetary instruments utilizing cryptocurrency accounts based at Virtual Currency Exchange A (“VC A”).

II. AGENT BACKGROUND

2. I am a Special Agent with Internal Revenue Service - Criminal Investigation Division (“IRS-CI”) and have been so employed since September 2014. As a Special Agent, my responsibilities include the investigation of criminal violations of the Internal Revenue Code (Title 26, United States Code), the Money Laundering Control Act (Title 18, United States Code), the

Bank Secrecy Act (Title 31, United States Code) and related offenses. I have a Bachelor of Business Administration in Accounting from Athens State University and a Master of Business Administration from Tennessee State University. I am a Certified Public Accountant, licensed in the state of Texas. I completed training at the National Criminal Investigation Training Academy at the Federal Law Enforcement Training Center in Glynco, Georgia. I completed the Criminal Investigator Training Program in December 2014, and the Special Agent Basic Training Program, conducted by the IRS's National Criminal Investigation Training Academy, in March 2015. I received extensive training in conducting financial investigations that involve analyzing books and records of individuals and businesses, such as journals, ledgers, bank accounts, invoices, receipts, and other records evidencing violations of the Internal Revenue Code and other financial crimes. I am currently assigned to the Cyber Crimes Unit in IRS-CI and I have received training in cyber operations and in criminal schemes perpetrated via the internet.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Because this affidavit is being submitted for a limited purpose, I have not set forth all of the information known to me concerning this investigation. Instead, I have set forth information that I believe to be sufficient to establish probable cause in support of this application for a criminal complaint. Where I have reported statements made by others, or from documents that I have reviewed, those statements are summarized, unless otherwise indicated.

4. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 1960 and Title 18, United States Code, Section 1956(h), have been committed by the defendants, Akti and Karataş.

III. JURISDICTION AND VENUE

5. As discussed more fully below, acts or omissions (*i.e.*, the failure to register with the Department of Treasury, Financial Crimes Enforcement Network (“FinCEN”)) in furtherance of the offenses under investigation, occurred within Washington, D.C. as well as the extraterritorial jurisdiction of this Court. *See* 18 U.S.C. §§ 3237, 1956(i)(2), and 1956(f).

IV. STATUTORY FRAMEWORK

A. Bank Secrecy Act and Violations of 18 U.S.C. § 1960

7. According to the U.S. Department of the Treasury, the global financial system, trade flows, and economic development, rely on correspondent banking relationships. To protect this system from abuse, U.S. financial institutions must comply with national anti-money laundering requirements set forth in the Bank Secrecy Act, codified at 31 U.S.C. § 5311 *et seq.* FinCEN is responsible for administering the Bank Secrecy Act in furtherance of its mission to safeguard the U.S. financial system from illicit use.

8. In addition to regulating U.S. financial institutions, the Bank Secrecy Act and FinCEN also regulate *foreign* financial institutions that either deal in foreign exchange or act as money transmitters in a manner that is not merely incidental to their businesses. *See* 31 C.F.R. 1010.605(f).

9. Title 18, United States Code, Section 1960 criminalizes certain violations of the Bank Secrecy Act. Specifically, it punishes money transmitting businesses,¹ in the U.S. and

¹ FINCEN uses the term “money service business” or MSB, to denote the companies that must register with the agency. Per its own definition, MSBs include “money transmitting businesses” and, specifically, those companies regulated by 18 U.S.C. § 1960.

abroad, that do not register with FinCEN pursuant to Section 5330 of the Bank Secrecy Act. *See* 18 U.S.C. § 1960 & 31 U.S.C. § 5330.

10. Under both 18 U.S.C. § 1960 and 31 U.S.C. § 5300, virtual currency exchangers qualify as money transmitting businesses and must thus comply with the Bank Secrecy Act. *See United States v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 87-97 (D.D.C. 2008). Indeed, the D.C. District Court has recently applied this statutory scheme and the Bank Secrecy Act, specifically to bitcoin-related businesses, ruling that bitcoin is “money,” and that a provider who moves bitcoin between individuals, virtual currency addresses, or locations, is operating a “money transmitting business” for purposes of 18 U.S.C. § 1960. *United States v. Harmon*, No. 19-CR-395 (BAH) (D.D.C. July 24, 2020) (ruling that bitcoin tumbler services qualify as MSBs and must comply with the Bank Secrecy Act).

11. FinCEN has issued formal guidance classifying virtual currency exchangers as MSBs, and thus subject to the federal registration requirement. *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), at 3 (“An administrator or exchanger that (1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency for any reason is a money transmitter under FinCEN’s regulations, unless a limitation to or exemption from the definition applies to the person.”) (emphasis in original). FinCEN has also issued subsequent guidance and rulings further regulating virtual currency exchangers, explaining that its regulations are essential to prevent an “MSB from being used to facilitate money laundering and the financing of terrorist activities.” *See* Dep’t of the Treasury FinCEN Guidance, Application of FinCEN’s Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2014-R007 at 9-10 (May 9, 2019); *see, e.g.*, Dep’t of the Treasury FinCEN Administrative

Ruling, Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform (Oct. 27, 2014), FIN-2014-R011; Dep't of the Treasury FinCEN Guidance, Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity (Jan. 30, 2014), FIN-2014-R002.

12. Virtual currency exchangers abroad are covered by 18 U.S.C. § 1960, and thereby must comply with the registrations requirements of 31 U.S.C. § 5300, if, as part of their money transmitting business, they “transfer[] funds on behalf of the public by any and all means including but *not limited to transfers within this country or to locations abroad by wire*, check, draft, facsimile, or courier.” *See* 18 U.S.C. § 1960(b)(2) (emphasis added). Notably, the statute explicitly contemplates the regulation of international transfers under its purview, defining “money transmitting businesses,” as those affecting “interstate *or foreign commerce*.” *See* 18 U.S.C. § 1960(b)(1) (emphasis added).

13. FinCEN has also issued formal guidance classifying “foreign entities” who engage in MSB “activities in the United States” as subject to the federal registration requirement. *See* Dep't of the Treasury FinCEN Guidance, FinCEN Clarifies Money Services Businesses Definitions Rule Includes Foreign-Located MSBs Doing Business in U.S., FIN-2011-3 (Jul. 18, 2011), at 1. “This requirement arose out of the recognition that the Internet and other technological advances make it increasingly possible for persons to offer MSB services in the United States from foreign locations.” *Id.* at 2.

B. Money Laundering

14. 18 U.S.C. § 1956(h) criminalizes a conspiracy to violate § 1956.

15. 18 U.S.C. § 1956(a)(2)(A) (the international promotional money laundering statute) criminalizes transporting, transmitting, and transferring, and attempting to transport, transmit, and

transfer a monetary instrument or funds to a place in the United States from or through a place outside the United States with the intent to promote the carrying on of specified unlawful activity.

16. Pursuant to 18 U.S.C. § 1956(c)(7)(A), the term “specified unlawful activity,” includes violations of 18 U.S.C. § 1960.

V. PROBABLE CAUSE

A. Background On Cryptocurrency

17. Bitcoin (BTC) and Ether (ETH) are pseudonymous virtual currencies. Although transactions are visible on a public ledger, each transaction is referenced by a complex series of numbers and letters (as opposed to identifiable individuals) involved in the transaction. The public ledger containing this series of numbers and letters is called a blockchain. This feature makes BTC and ETH pseudonymous; however, it is often possible to determine the identity of an individual involved in BTC and ETH transactions through several different tools. For this reason, many criminal actors who use BTC and ETH to facilitate illicit transactions online (*e.g.*, to buy and sell drugs or other illegal items or services) look for avenues to make their transactions even more anonymous. BTC/ETH addresses are unique tokens; however, BTC/ETH are designed such that one person may easily operate many accounts or addresses at one time. Like an email address, a user can send to, and receive BTC/ETH from, others by sending BTC/ETH to a BTC/ETH address. In my training and experience, I know that individuals commonly have many different addresses, and an individual could theoretically use a unique address for every transaction in which he/she engages.

18. A BTC/ETH user can also combine multiple BTC/ETH addresses in one transaction. To spend BTC/ETH held within a BTC/ETH address, however, the user must have a private key, which is generated when the BTC/ETH address is created. Similar to a password, a

private key is shared only with the BTC/ETH-address key's initiator and ensures secured access to the virtual currency. Consequently, only the holder of a private key for a BTC/ETH address can spend BTC/ETH from the address.

19. Although as a general matter, the owners of BTC/ETH addresses are not known unless the information is made public by the owner (for example, by posting the address in an online forum or providing the BTC/ETH address to another user for a transaction), analyzing the public transaction ledger can sometimes lead to the identification of both the owner of an address and any other accounts controlled by the same individual.

20. While the identity of the BTC/ETH address owner is generally anonymous (unless the owner opts to make the information publicly available as described above), law enforcement can identify the owner of a particular address by analyzing the blockchain. The analysis can also reveal additional addresses controlled by the same individual or entity. For example, a user or business may create many BTC/ETH addresses to receive payments from different customers. When the user wants to transact the BTC/ETH that it has received (for example, to exchange BTC/ETH for other currency or to purchase goods or services), it may group those addresses together to send a single transaction. Law enforcement uses commercial services offered by several different blockchain-analysis companies to investigate virtual currency transactions. These companies analyze the blockchain and attempt to identify the individuals or groups involved in the virtual currency transactions. Specifically, these companies create large databases that group transactions into "clusters" through analysis of data underlying the virtual currency transactions.

21. BTC/ETH are often transacted using a virtual currency exchange, which provides trading and BTC/ETH storage services. An exchange typically allows trading between the U.S. dollar, foreign fiat currencies, BTC, ETH, and other virtual currencies. Many virtual currency

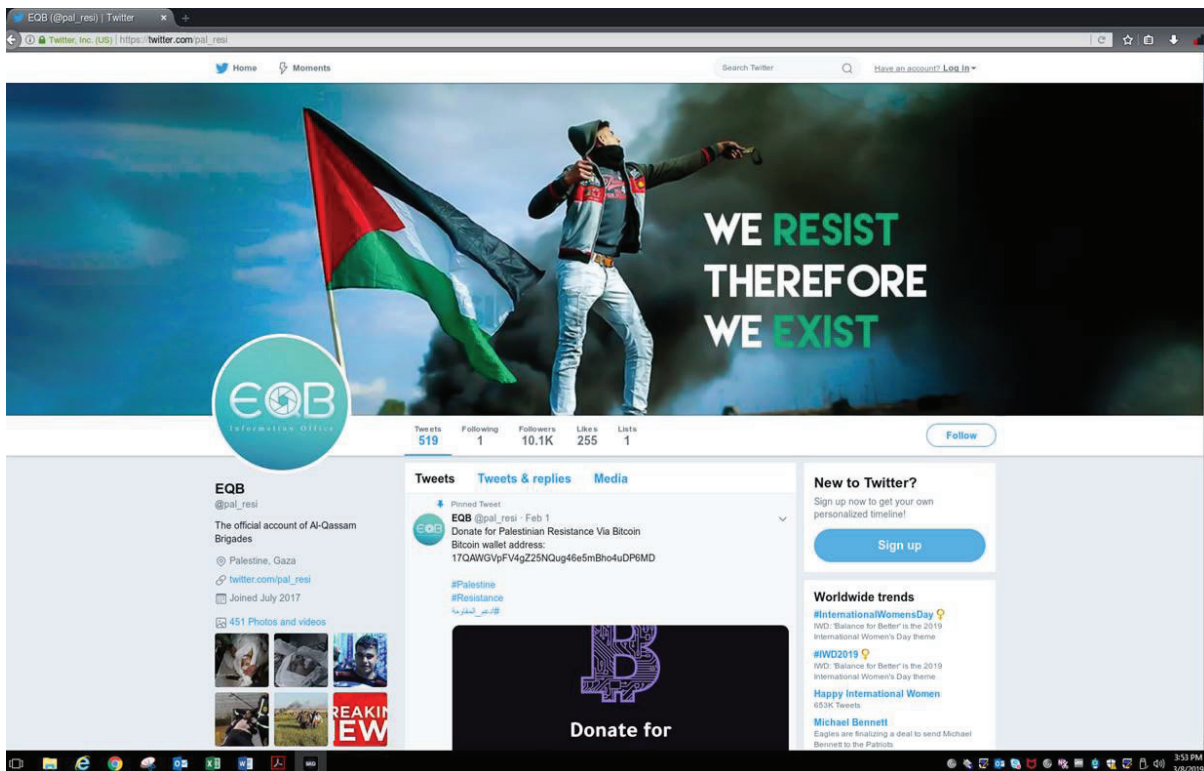
exchanges also store their customers' virtual currencies. In my training and experience, I know that in these roles, the exchanges act as money transmitting businesses and are, thus, legally required to conduct due diligence of their customers and implement anti-money laundering checks. More specifically, virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act, codified at 31 U.S.C. § 5311 *et seq.*, and must collect identifying information of their customers and verify their clients' identities. *See United States v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 87-97 (D.D.C. 2008). As such, in my experience, if an individual is relying on virtual currency exchanges to host a BTC/ETH address, it is usually possible to secure identifying information from the exchange itself that it secured via KYC compliance.

22. BTC/ETH are just two of the virtual currencies and tokens available for trading on most virtual currency exchanges. Some of the other major virtual currencies, based on market capitalization, include Ripple (XRP), EOS, Tether (USDT), BSV, Stellar (XLM), and LEO.

B. Hamas and The al-Qassam Brigades' Fundraising Campaign

23. On October 8, 1997, by publication in the Federal Register, the United States Secretary of State designated Hamas as a Foreign Terrorist Organization ("FTO") pursuant to Section 219 of the Immigration and Nationality Act. On October 31, 2001, the Secretary of State also designated Hamas as a Specially Designated Global Terrorist under Executive Order 13224. As part of this designation, the Secretary of State listed a number of aliases for HAMAS, including, Izz Al-Din Al-Qassim Brigades, Izz Al-Din Al-Qassim Forces, Izz Al-Din Al Qassim Battalions, Izz al-Din Al Qassam Brigades, Izz al-Din Al Qassam Forces, and Izz al-Din Al Qassam Battalions. I am aware that to date, Hamas remains a designated FTO and the al-Qassam Brigades persists as the powerful military branch of Hamas.

24. In January 2019, the al-Qassam Brigades began a fundraising campaign on social media to solicit BTC donations from supporters. To receive BTC donations, the organization created multiple cryptocurrency accounts, including one beginning with 17QAW that the organization publicly posted on its social media accounts. The campaign asked donors to send BTC to its accounts, included to 17QAW, as shown below:



25. Using the techniques described *supra* paragraph 18, law enforcement clustered 17QAW with ten other BTC addresses, which together comprised “ Hamas Account 2.” In my training and experience, I know that the “clustering” of accounts indicates common ownership and control.

26. Hamas Account 2 received a number of donations from supporters for the terrorist fundraising campaign, before the al-Qassam Brigades shifted its BTC fundraising campaign to its official websites, “alqassam.net” and “alqassam.ps.” The website campaign relied on unique BTC addresses generated for each donor, rather than requesting direct donations to Hamas Account 2.

C. Involvement of Defendant Mehmet Akti

27. Once the Hamas accounts and addresses amassed BTC from fundraising efforts, law enforcement determined through blockchain analysis, that the accounts typically converted the virtual currency to traditional fiat currency or exchanged it for something of value, such as a gift card, so that the al-Qassam Brigades could spend the funds on its terror campaign. Using blockchain analysis, law enforcement also traced at least one transaction from Hamas Account 2 to Akti's account at VC A ("VC Account 1").

28. Specifically, on February 14, 2019, Hamas sent approximately 0.066 BTC (valued at approximately \$227.48 as of the date of this transaction) from Hamas Account 2 to an intermediary BTC deposit address. Within a few hours, that intermediary address transferred approximately 0.069 BTC to VC Account 1 at VC A. VC A records showed that VC Account 1 utilizes a BTC deposit address starting with 15LD. These records also revealed that the account was registered to Akti on October 16, 2017.

29. In response to a VC A "know your customer" ("KYC") inquiry, Akti wrote to VC A on or about March 8, 2019, that he used his account for the "purchase and sale of cryptocurrency, as well as the provision of services related to this activity." Law enforcement determined that at the time of this statement, and at all times relevant to the conduct alleged, Akti was not registered with FINCEN as a MSB.

30. In spite of this lack of registration, VC A records demonstrate that Akti operated a prolific virtual currency MSB from his account. Specifically, between October 2017 and March 2019, VC Account 1 was in receipt of approximately 2,328 BTC, 2,296 ETH, and U.S. dollar wires totaling \$82.8 million. All of the U.S. dollar wires originated from a Turkish bank account held in the name Deniz Royal Dis Ticaret Limited Sirketi ("Deniz Royal"). Due to the nature of

correspondent bank transactions, these international wires transited from outside the United States into the United States and then back out to the intended destination. VC A records show Akti then used these U.S. dollar wires to acquire additional virtual currencies, primarily BTC and ETH.

31. During the same period, Akti withdrew large amounts of virtual currency from VC Account 1, to include approximately 11,228 BTC, 7,063 ETH, 957,109 XRP, and 118,008 EOS. Notably, these withdrawals were sent to over 250 unique cryptocurrency wallet addresses and involved transactions totaling over \$90 million, suggesting that Akti had hundreds of customers for whom he transmitted money, as an unlicensed MSB.

32. VC A records further show that at least six of Akti's customers lived in the United States at the time of the transactions or relied on an account at a U.S.-based virtual currency exchange to use Akti's services. In total, Akti sent these U.S. nexus customers, approximately 373 BTC from VC Account 1, as part of his unlicensed money transmitting business.

a. For example, on or about June 28, 2018, Akti withdrew approximately 3.26 BTC from VC Account 1, depositing it to a BTC address starting with 38td ("Wallet 38td"). Blockchain analysis revealed that Wallet 38td was associated with an account held at U.S. Exchange 1. Subpoena returns from U.S. Exchange 1 showed that Wallet 38td was associated with an account opened on December 7, 2017, by Customer 1 in the United States. Customer 1 told law enforcement that Customer 1 did not know Akti and had received funds from individuals who relied on money transmitter services in Gaza, Palestine.

D. Liquidation of VC Account 1

33. Following Akti's statement to VC A in March 2019 that he was purchasing and selling cryptocurrency, Akti liquidated VC Account 1, and transferred almost all of his virtual currency assets to other wallets.

34. Over the following four weeks, almost half of this cryptocurrency was redeposited into a second account at VC A (“VC Account 2”) that was registered to Defendant Karataş. Notably, Karataş opened VC Account 2 on March 20, 2019, nearly the same time as Akti’s liquidation. In total, approximately 42.2 BTC, 2,465 ETH, 123,500 XRP, and 70,055 EOS (approximately \$803,712, collectively at the time) was transferred from Akti’s VC Account 1 to Karataş’ VC Account 2.

E. Involvement of Defendant Hüsametdin Karataş

35. As part of the money laundering investigation, law enforcement interviewed Karataş, who was represented by counsel. Karataş stated in a signed affidavit that:

a. Akti was a cryptocurrency broker. Karataş was not related to Akti, and Karataş claimed he was not business partners with Akti.

b. Akti supposedly purchased the virtual currency assets, which were transferred from VC Account 1 to VC Account 2, on behalf of Karataş. Karataş claimed that he gave Akti “cash in hand” with which to acquire these virtual currency assets. Karataş did not have any documentation, receipts, agreements or bank statements to support this activity.

c. Karataş claimed that for a period of time, Akti stored Karataş’ virtual currency assets in VC Account 1 for no fees, because Karataş did not have his own account. Karataş could provide no explanation as to why he was unable to open a virtual currency account at that earlier time, or why he was able to do so later. Karataş also could not explain why Akti would have provided him this free service.

d. In early 2019, Akti purportedly told Karataş that Akti was closing VC Account 1. As a result, Karataş opened VC Account 2 and requested Akti move Karataş’s virtual

currency assets into this account. Karatas claimed in his affidavit that he had no contact with Akti after April 2019.

e. Karataş then told law enforcement that once he opened VC Account 2, he began selling his own cryptocurrency assets, thereby admitting to knowingly operating an MSB.

36. Further investigation into Karataş and VC Account 2 confirmed that he operated a MSB out of VC Account 2. In addition to the cryptocurrency received from Akti, Karataş received cryptocurrency and fiat currency valued at approximately \$2.1 million dollars into VC Account 2 between in or about April 2019 through in or about July 2019. This included \$500,000 in U.S. wires from Deniz Royal, the same company that sent \$82.8 million in U.S. wires to Akti at VC Account 1.

37. During this same time period, Karataş withdrew cryptocurrency valued at approximately \$2.3 million dollars to approximately 17 unique wallet addresses.

38. One of Karataş's customers transacted with Karataş on a U.S.-based virtual currency exchange. In total, this customer, with a U.S. nexus, received approximately 19,290 USDT from Karataş's account at VC A. This same customer previously transacted with Akti in the amount of 2 BTC.

39. Despite these transactions in U.S. dollar wires and with U.S.-based virtual currency exchanges, I am aware that at all relevant times, Karatas was not registered with FinCEN as an MSB.

F. Connections Between Akti and Karatas

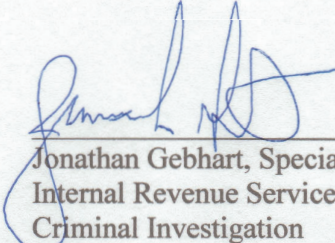
40. Akti and Karatas's MSB shared a number of customers, including Deniz Royal, discussed above, a customer transacting on a U.S. based virtual currency exchange, discussed

above, and a Ukrainian national who sent almost one million dollars of different currencies to VC Account 1 and VC Account 2 in 2019.

41. Their businesses and accounts at VC A were also linked through IP addresses. Specifically, records from VC A showed that a mobile device utilizing the same IP address, same operating system version, and same browser version logged into both VC Account 1 and VC Account 2 within minutes of each other on May 9, 2019, May 14, 2019, and August 28, 2019. One of these IP addresses linking the accounts at VC A, was the primary IP address utilized to access both accounts: It was used on approximately 284 occasions to access VC Account 1 between January 2018 and August 2019, and on approximately 85 occasions to access VC Account 2 between March 2019 and September 2019.

VI. CONCLUSION

42. In summary, based upon the above facts and information, I submit that there is probable cause to believe that Akti and Karataş have violated 18 U.S.C. §§ 1960 and 1956(h).


Jonathan Gebhart, Special Agent
Internal Revenue Service
Criminal Investigation

Subscribed and sworn pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) on this 12th day of August, 2020.




2020.08.12
12:28:54 -04'00'

THE HONORABLE G. MICHAEL HARVEY
UNITED STATES MAGISTRATE JUDGE