

UNITED STATES DISTRICT COURT  
DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA

-- v. --

SAUL SHALEV,

Defendant.

Case No.

**Filed Under Seal**

**AFFIDAVIT**

I, Michael Stempien, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of the Government's application for a warrant to arrest SAUL SHALEV, who is believed to be a citizen of the United States of America residing in Israel. This affidavit is submitted for the purpose of establishing probable cause to believe that SHALEV committed wire fraud, money laundering, and aggravated identity theft, in violation of Title 18, United States Code, Sections 1343, 1956(a)(1)(B)(i), 1028A, and 2, respectively.

2. The facts set forth in this affidavit are based on information that I have obtained from my personal involvement in the investigation and from other law enforcement officers who have been involved in this investigation, on documents that I have reviewed, and on my training and experience. Where the contents of documents or communications with others are reported herein, they are reported in substance and in part. Because this affidavit is being submitted for limited purposes, 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 the Government's application for an arrest warrant.

3. I am, and have been, a Task Force Officer with the Federal Bureau of Investigation ("FBI") since 2017 and a Detective with the Stamford Police Department since

2006. Since 2011, I have been assigned to the Stamford Police Bureau of Criminal Investigations Financial Crimes Unit. In addition to that role, since October of 2017, I have been assigned to the FBI New Haven Division Cyber Task Force. In my law enforcement experience, I have handled numerous investigations involving wire fraud and computer crimes. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, software, and electronically stored information. I have also received formal and informal training from the FBI, Stamford Police Department, and other institutions on the investigation of financial fraud and cyber crimes. Since approximately 2013, I have held certification as an instructor for the subject of Property Crimes/Financial Crimes through the Connecticut Police Officer Standards and Training Council. In addition to my training through the FBI and Stamford Police, in 2018 I obtained a Master of Science in Financial Crime and Compliance Management from Utica College.

### **PROBABLE CAUSE**

#### **The Scheme to Defraud**

4. As described more fully below, there is probable cause to believe that one or more individuals, including an individual named SAUL SHALEV, have conducted a fraud scheme with business victims in Connecticut and throughout the United States. Over 25 victims of the scheme have been identified, starting as early as 2020 and continuing as recently as February 2025 .

5. In broad strokes, the scheme operated by deceiving the business victims into believing that they were re-financing an original loan from a certain financial institution (the “Original Lender”) or obtaining a new loan from another lender. In order to execute the scheme, the subject(s) of the investigation used stolen identities and personally identifiable information

(PII) to pose (i) as authorized representatives or agents of the financial institutions when communicating with a victim, and (ii) as officers or employees of a victim when communicating with the financial institutions. Once a victim received proceeds from a new or re-financed loan, the subject(s) of the investigation would direct the victim to use a portion of the proceeds to pay off its loan from the Original Lender; or, alternatively, would inform the victim that a wiring error had occurred and direct the victim to return the funds in order to correct the error. In fact, however, the payment instructions would cause the funds to be sent to the subject(s) of the investigation. The subject(s) of the investigation also fraudulently received commissions from the financial institutions. The proceeds of the scheme, *i.e.*, the mis-directed funds and the commissions, were laundered by being converted into different forms of cryptocurrency.

6. I have interviewed employees from numerous businesses and financial institutions that were victims of the scheme, and I have reviewed bank records, correspondence, and other documents that substantiate the scheme described above. The scheme has been executed, for example, against a loan company in Greenwich, Connecticut (“New Lender 1”) in connection with a loan to a business in Ohio (“Company 1”), both of whose identities are known to me:

- a. According to information provided by New Lender 1 in a police report, in or about December 2020, New Lender 1 began communicating with an individual purporting to represent Company 1 as a broker. After receiving loan application materials and communicating with an individual who purported to be the owner of Company 1, New Lender 1 transferred approximately \$343,000 to Company 1 and a commission of \$42,000 to the purported broker.
- b. According to information provided by Company 1, its owner was communicating with somebody purporting to represent Original Lender, to whom Company 1 had

an outstanding debt of approximately \$190,668. The owner of Company 1 was led to believe that he could re-negotiate his loan with the Original Lender, with part of the proceeds being used to pay off the existing loan. Upon receiving the \$343,000 from New Lender 1, Company 1 wired \$190,668 to an account that was represented to belong to the Original Lender.

- c. Records obtained from First Internet Bank (“FI Bank”) show that, on or about December 28, 2020, the payment of approximately \$190,668 from Company 1 was received by FI Bank account ‘8051. According to information provided by the Original Lender, it was not associated with this account and did not receive this payment. Records obtained from FI Bank also show that, on or about December 29, 2020, the commission of \$42,000 from New Lender 1 was received by FI Bank account ‘9529, then transferred the same day to FI Bank account ‘8051. As described more fully below, both sums were then transferred from FI Bank to the cryptocurrency exchange SFOX.

#### Aggravated Identity Theft

7. In executing the scheme against Company 1 and New Lender 1, the subject(s) of the investigation used numerous stolen identities.
  - a. In order to act as a broker for New Lender 1, the subject(s) used the identity of an individual with initials S.K. In particular, on or about December 17, 2020, in an email message to New Lender 1, the subject(s) sent New Lender 1 a copy of a New York driver’s license for S.K. According to the actual S.K., whom I interviewed, the driver’s license in fact belonged to him but he did not work as a loan broker and had no involvement with New Lender 1.

- b. In order to open FI Bank account '9529, on or about December 14, 2020, the subject(s) used the identity of an individual with initials J.A., including the individual's date of birth and Social Security account number. According to the actual J.A., whom I interviewed, he has never opened an account at FI Bank nor authorized anybody else to do so on his behalf.

#### Money Laundering

8. As described above, proceeds of the fraud scheme executed against Company 1 and New Lender 1 – in the amounts of approximately \$190,668 and \$42,000 – were deposited or transferred to FI Bank account '8051 in December 2020. According to records provided by FI Bank, the account started the month with a zero balance. During the month, three wire transfers were made from the account to the cryptocurrency exchange SFOX in the total amount of \$254,250. (Of that amount, therefore, approximately 91.51% can be attributed to the proceeds of the fraud against Company 1 and New Lender 1.) The account ended the month with a balance of approximately \$58 dollars and was closed the following month.

9. According to records provided by SFOX, the three incoming wires resulted in the purchase of approximately 9.56459779 in bitcoin (BTC). From on or about December 22, 2020 through on or about January 7, 2021, all of the bitcoin was withdrawn.

10. According to publicly available records on the bitcoin blockchain, together with records from a cryptocurrency service whose identity is known to me (the "Crypto Service"), almost all of the bitcoin – approximately 9.54937972 BTC – was traceable to the Crypto Service. Of that amount, on or about December 29 and December 30, 2020, 3.565598 BTC was converted to a cryptocurrency that was not further traced. On or about February 18, 2021, the remaining 5.99506195 BTC was converted to approximately 156.634467 Ethereum (ETH).

11. According to publicly available records on the Ethereum blockchain, on or about February 18, 2021, the Ethereum was converted to Frontier (FRONT) tokens.

12. According to publicly available records on the Ethereum blockchain, together with records from the Crypto Service, on or about October 23, 2021, the Frontier tokens were converted to Ethereum.

13. According to publicly available records on the Ethereum blockchain, on or about October 26, 2021, the Ethereum tokens were converted to Liquity tokens (LUSD), which were converted to the Tether cryptocurrency (USDT) and transferred in a transaction associated with the hash value ending in '5c5cb.

14. According to records provided by Paxful, a cryptocurrency exchange, the USDT involved in the '5c5cb transaction was credited to an account in the name of Saul Shalev, with the user name "Milleniumtrust," and the email address saulshalev@gmail.com (the "Paxful Account"). The Paxful records also show that there are two bank accounts associated with the Paxful Account, including Citibank account '0685 and Capital One account '6403, both in the name of "Saul Shalev."

15. Records provided by Citibank and Capital One confirm that Citibank account '0685 and Capital One account '6403 were opened in the name of Saul Shalev, with an address of 1538 E. 4th St. in Brooklyn, New York. The email addresses associated with the accounts were milleniumtrustcapital@gmail.com and saulshalev8@gmail.com, respectively.

16. From the time the fraud proceeds were withdrawn from SFOX until the time they reached the Paxful Account, all of the transactions described above were conducted anonymously.

Additional Attribution Evidence

17. In addition to the tracing of the proceeds of the fraud to the Paxful Account in SHALEV's name, there is additional evidence supporting probable cause to believe that SHALEV was involved in executing the scheme to defraud based on IP address analysis. In particular, during the course of executing the scheme to defraud, the subject(s) of the investigation purchased several internet domain names that were similar to the internet domain name of the Original Lender. One such domain name was the name of the Original Lender followed by ".us.com" (the "Fraudulent Domain"). According to publicly available records, the Fraudulent Domain was registered through Namecheap, Inc.

18. According to records provided by Namecheap, the Fraudulent Domain was registered by "Brian Soloway." This was the name of the alleged employee at the Original Lender used by the subject(s) of the investigation to communicate with Company 1 while perpetrating the fraud.

19. On at least three occasions, the Namecheap account used to register the Fraudulent Domain was accessed from the same IP address, at approximately the same time, that was used to access an online financial account in SHALEV's name. According to records provided by Namecheap, Wise US, Inc., and Citibank:

- a. On March 6, 2020, at 11:05 a.m., the Namecheap account used to register the Fraudulent Domain was accessed from IP address 89.187.177.227. The same IP address was used to access a Wise account, in the name of Saul Shalev, at 3:57 p.m. The address associated with the account was 1538 E. 4th St. in Brooklyn, New York.

- b. On November 17, 2020, at 2:00 p.m., the Namecheap account used to register the Fraudulent Domain was accessed from IP address 172.98.93.166. The same IP address was used to access Citibank account '0685 at 2:19 p.m.
- c. On November 25, 2020, at 9:07:10 a.m., the Namecheap account used to register the Fraudulent Domain was accessed from IP address 89.187.178.22. The same IP address was used to access Citibank account '0685 at 9:57 a.m.

20. Probable cause is further supported by email messages found in SHALEV's

Google accounts. In particular:

- a. On or about December 2, 2019, the account "milleniumtrustcapital@gmail.com" received an email message from DocuSign. DocuSign is a service that allows multiple parties to electronically sign documents, and it was used to perpetrate the fraud against Company 1 and other identified victims. In this email message, DocuSign was providing confirmation on behalf of "Brian Soloway," with an email address at the Fraudulent Domain, that a document named "Authorization Form.pdf" had been completed by all parties.
- b. On or about March 12, 2020, the account "saulshalev@gmail.com" includes an email message sent to itself, from "Saul Shalev" to "Saul Shalev," with the subject line "raw" and no body. The email included three spreadsheets as attachments, which appear to contain the names of businesses, UCC filing numbers, and lender information. One of the spreadsheets lists Company 1 and the Original Lender. There is probable cause to believe that this information was used to identify businesses with outstanding loans, such as Company 1, that were targeted by the subject(s) of the investigation.

- c. On or about March 17, 2020, the account “saushalev@gmail.com” includes an email message sent to itself, from “Saul Shalev” to “Saul Shalev,” that has no subject line and no body. The email includes an attachment titled “Billing – RingCentral.pdf.” The attachment appears to be an invoice from the phone service provider RingCentral relating to the telephone number (415)813-5887. Records provided by RingCentral confirm the existence of an account associated with that telephone number. Furthermore, that telephone number was used to communicate with Company 1 in order to perpetrate the scheme to defraud.

Identification of Saul Shalev

21. According to records provided by Paxful, the “know your customer” records for the Paxful Account include photographs of SHALEV and his United States passport, as cropped and shown in Attachment A to this affidavit.

22. According to records of United States Customs and Border Protection, SHALEV departed the United States for Israel on or about February 24, 2019, and has not returned since.

23. According to records provided by Google, on or about March 17, 2020, the account saushalev@gmail.com received an email message with the subject line “Receipt Rent Payments.” The email included an attachment that appeared to be a receipt for rent payments from April 2020 to March 2021 for Rothschild 36, apt 202, in Tel Aviv, Israel.

24. According to records provided by Google, on or about April 11, 2021, the account saushalev@gmail.com sent an email message to bshalev@aol.com with the subject line “Nonsense” and no body. The email included an attachment that appears to be a copy of SHALEV’s Israeli passport, as cropped and shown in Attachment A to this affidavit.

25. Based on the foregoing, there is probable cause to believe that SHALEV committed wire fraud, in violation of Title 18, United States Code, Sections 1343 and 2. In particular, on or about December 29, 2020, SHALEV caused New Lender 1, located in Greenwich, Connecticut, to fraudulently transfer a commission of \$42,000 to an account at First Internet Bank, located in Fishers, Indiana.

26. There is further probable cause to believe that SHALEV committed aggravated identity theft, in violation of Title 18, United States Code, Sections 1028A and 2. In particular, SHALEV used without lawful authority means of identification of S.K. and J.A. in furtherance of the scheme to defraud.

27. Finally, there is probable cause to believe that SHALEV engaged in money laundering, in violation of Title 18, United States Code, Sections 1956(a)(1)(B)(i) and 2. In particular, SHALEV transferred and converted the proceeds of the scheme to defraud into various forms of cryptocurrency before eventually depositing the proceeds into the Paxful Account, an account in his own name.

### **STATUTORY AUTHORITY**

#### **Wire Fraud**

28. Title 18, United States Code, Section 1343 provides:

Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire . . . communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall [be guilty of a crime].

Aggravated Identity Theft

29. Title 18, United States Code, Section 1028A provides:

Whoever, during and in relation to [specified violations including wire fraud], knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person shall [be guilty of a crime].

Money Laundering

30. Title 18, United States Code, Section 1956(a)(1) provides:

Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(A) . . .

(B) knowing that the transaction is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity [shall be guilty of a crime].

Aiding and Abetting

31. Title 18, United States Code, Section 2 provides:

- (a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.
- (b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.

**CONCLUSION**

32. Based on the forgoing, I respectfully request that the Court issue a warrant authorizing the arrest of SAUL SHALEV.

Respectfully submitted,



---

MICHAEL STEMPIEN  
Task Force Officer, FBI

The truth of the foregoing affidavit has been attested to me by Task Force Officer Michael Stempien on this 24th day of February, 2025.



---

HONORABLE S. DAVE VATTI  
UNITED STATES MAGISTRATE JUDGE

