9

AUSA: Timothy Wyse Telephone: (313) 226-9144

AO 91 (Rev. 11/11) Criminal Complaint Agent: Mark Koch Telephone: (313) 226-5033

UNITED STATES DISTRICT COURT

for the

Eastern District of Michigan

United States of America
v.

D-1 Jarratt White
D-2 Robert Jack
D-3 Fendley Joseph

Case:2:19-mj-30227
Judge: Unassigned,
Filed: 05-02-2019 At 11:51 AM
IN RE:SEALED MATTER(CMP)(MLW)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of May 2018 in the county of Wayne in the Eastern District of Michigan, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §1343- Wire Fraud	
~~18 U.S.C. 1349-Conspiracy to Commit Wire Fraud~~	
~~18 U.S.C. § 1028A(a)(1)-Aggravated Identify~~ Theft	

This criminal complaint is based on these facts:

Please see attached affidavit.

☑ Continued on the attached sheet.

Complainant's signature

Mark Koch - Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: May 2, 2019

Judge's signature

City and state: Detroit, Michigan

Anthony P. Patti- U.S Magistrate Judge
Printed name and title

AFFIDAVIT

Mark MRK

~~March~~ R. Koch, being duly sworn, deposes and states:

1. I am a Special Agent with Homeland Security Investigations (HSI), Detroit, Michigan, and have been so employed for fifteen years. My duties include investigating computer crimes and financial crimes. The allegations contained in this affidavit are based on the review of records and HSI interviews. Because this affidavit is being submitted for the limited purpose of establishing probable cause for a criminal complaint, I have not included every detail of every aspect of the investigation. Rather, I have set forth only those facts that I believe are necessary to establish probable cause that JARRATT WHITE, ROBERT JACK, and FENDLEY JOSEPH knowingly participated in a scheme to defraud through the transmission of wire communication in interstate commerce for the purpose of executing the scheme, in violation of 18 U.S.C. §1343. All conversations and statements described in this affidavit are related in substance and in part, and are not verbatim quotations.

BACKGROUND ON "THE COMMUNITY"

2. "The Community" was a loosely organized group of individuals dedicated to online identity theft. A subset of The Community focused on the theft of cryptocurrencies such as Bitcoin, LiteCoin, and Ethereum.

3. Members of The Community planned and organized their activities on online forums and over diverse channels of communication. Broader discussions—such as discussing the manner and means of attacks generally, and networking among The Community's members—typically took place on forums such as "OGUsers" and "Hackforums." Planning and execution of specific attacks, as well as victim selection and recruiting, usually took place via platforms such as Discord, Skype, Signal, Wickr, and Telegram.

4. The Community engaged in "SIM Hijacking," or "SIM Swapping." This tactic enabled The Community to gain control of a victim's mobile phone number by linking that number to a subscriber identity module ("SIM") card controlled by The Community—resulting in the victim's phone calls and short message service ("SMS") messages being routed to a device controlled by a member of The Community.

5. Once The Community had control of a victim's phone number, it was leveraged as a gateway to gain control of online accounts such as the victim's email, cloud storage, and cryptocurrency exchange accounts.

Sometimes this was achieved by requesting a password-reset link be sent via SMS to the device controlled by The Community. Sometimes passwords were compromised by other means, and The Community's device was used to receive two-factor authentication ("2FA") messages sent via SMS intended for the victim.

6. Specific members of The Community endeavored to gain control of a victim's cryptocurrency wallet or online cryptocurrency exchange account and steal the victim's funds. Stolen funds from a successful attack were divided among members of The Community that participated in that attack.

7. During these attacks, one or more members of The Community would appropriate the online identity of the victim, using means of identification including the victim's name, email, and mobile phone number.

8. SIM Hijacking was often facilitated by bribing an employee of a mobile phone provider. These employees, while not necessarily knowing the entirety of The Community's plans, were aware that they were assisting in the theft of identities of subscribers to their employer's services.

9. On April 18, 2019, six members of The Community were indicted by a grand jury in the Eastern District of Michigan on charges of Wire Fraud (18 U.S.C. 1343), Conspiracy to Commit Wire Fraud (18 U.S.C. 1349), and Aggravated Identify Theft (18 U.S.C. § 1028A(a)(1))

JARRATT WHITE

10. JARRATT WHITE is a former contract employee of AT&T residing in Arizona. He was repeatedly bribed by JD, a member of The Community, to assist The Community with their attacks.

11. WHITE's support is linked to the thefts from victims JP ($1,669.56), AL ($55,493.76), SS ($1,921,335.80), and MT ($164,972.47). In total, WHITE's assistance facilitated the theft of approximately $2,143,471.59.

12. JD communicated with WHITE via Telegram; WHITE used the handle ".O." Records from LocalBitcoins.com (a site that JD used to pay WHITE by way of PayPal) and PayPal demonstrate that JD paid a total of approximately $4,300 in May 2018 to a PayPal account associated with the email address Jarrattw@gmail.com. User information provided by PayPal linked this account to JARRATT WHITE of Tucson, Arizona.

13. In an interview with HSI, JD described his interaction and payments to ".O." JD recalled that .O was an employee associated with AT&T and that his first name started with "J."

14. Communications from JD to WHITE, as well as the payments made to WHITE, travelled via wire in interstate commerce originating in the Eastern District of Michigan.

15. AT&T confirmed that WHITE was a contract employee from Tucson, Arizona. They also provided data that confirmed that WHITE conducted twenty-nine unauthorized SIM swaps in May of 2018—including the swaps that facilitated the thefts from JP, AL, and MT.

ROBERT JACK

16. Based on records provided from AT&T, ROBERT JACK, a second AT&T contract employee from Tucson, Arizona, conducted twelve unauthorized SIM swaps in May of 2018—including the swap that facilitated the theft from victim SS.

17. Based on review of financial transactions and interviews with JD, the combined forty-one swaps that were conducted by WHITE and JACK match up approximately with the payments JD made to WHITE.

18. Review of social media indicates that JACK is an associate of WHITE.

19. PayPal payments have been identified made by WHITE to JACK that are near simultaneous to bribes paid to WHITE by JD. In total, WHITE paid JACK approximately $585.25 that has been linked to attacks by The Community.

FENDLEY JOSEPH

20. FENDLEY JOSEPH was an employee of Verizon residing in Murrietta, California who was also bribed by JD to assist The Community. Joseph's assistance facilitated the theft of approximately $100,000 from victim DM.

21. JOSEPH did not personally swap phone numbers for JD. Instead, JD paid JOSEPH to provide Personal Identifiable Information (PII) for targeted Verizon customers. With the PII that JOSEPH provided, JD or another member of The Community would then call Verizon and impersonate the target—requesting that the target's phone number be reassigned to a device controlled by The Community.

22. JD communicated with JOSEPH via Telegram; JOSEPH used the handle "Joseph Fin." According to JD, this individual was the only Verizon employee on his payroll.

23. Records from Local Bitcoins and PayPal demonstrate that in May of 2018 JD paid $3,500 to the PayPal user "fendleyvzw@gmail.com." Records from PayPal associate this user with the name "Mike James," a phone number ending in 1928, and a Suntrust Bank account ending in 8436.

24. Mike James is an alias—records from Verizon link the phone number and the bank account provided by PayPal to their employee FENDLEY JOSEPH.

25. Records from Google associate the "fendleyvzw" Gmail account with "Fendley Joseph."

26. Communications from JD to JOSEPH, as well as the payments made to JOSEPH, travelled via wire in interstate commerce originating in the Eastern District of Michigan.

CONCLUSION

27. Based on the aforementioned information, affiant believes that probable cause exists that in or about May of 2018, in the Eastern District of Michigan and elsewhere, JARRATT WHITE, ROBERT JACK, and FENDLEY JOSEPH knowingly and willfully participated in a scheme to defraud through the transmission wire communication in interstate commerce for the purpose of executing said scheme. Based upon the foregoing facts, there is probable cause to believe that JARRATT WHITE, ROBERT JACK, and FENDLEY JOSEPH committed wire fraud in violation of Title 18, United States Code, Section 1343.

Mark R. Koch, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me

This 2nd Day of May 2019.

Honorable Anthony P. Patti
United States Magistrate Judge