AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, Eric Preston, being duly sworn, state as follows:

Qualifications

1. I am a Special Agent with the Federal Bureau of Investigation (FBI). I am currently assigned to the FBI Cyber Division (CyD) in Washington, D.C., and have been employed since March 2015. As a Apecial Agent, my primary duty has been to investigate violations of state and federal law, including computer fraud, identity theft, and violations of Title 18 of the United States Code. I also have experience in over forty investigations and have conducted or participated in arrests, the execution of search warrants, and digital surveillance. I have training in digital forensics, data analysis and preservation, encryption, and cybercriminal tactics.

PURPOSE OF AFFIDAVIT

The Crime

2. I make this affidavit in support of a Search and Seizure warrant alleging that LEON GILL, has violated the following federal statutes:

    a. 18 U.S.C. § 1028 – Fraud and related activity in connection with identification documents, authentication features, and information;
    b. 18 U.S.C. § 1028A – Aggravated identity theft;
    c. 18 U.S.C. § 1030(a)(2)(A) - Intentionally obtaining unauthorized information within a financial record, card issuer, or a consumer reporting agency file as defined in the Fair Credit Reporting Act.

3. Based on the following facts, there is probable cause to believe that the residence of LEON GILL contains evidence, contraband, fruits of crime, or other items in violation of 18 U.S.C. § § 1028, 1028A, and 1030(a)(2)(A).
4. Regarding specific evidence, it is believed that LEON GILL has obtained financial account information, Social Security Numbers (SSNs), credit card numbers, and passwords and has used this evidence from multiple victims to make large purchases in their respective names in the commission of identity fraud. The facts in this affidavit come from my personal training and experience, surveillance footage, information from interviewing victims, publicly available records, social media posts, and metadata analysis. Because this affidavit is for the limited purpose of establishing probable cause, it does not cover every fact learned throughout this investigation.

PROBABLE CAUSE

Facts and Circumstances Supporting Probable Cause

5. On or about January 7, 2025, the FBI began receiving an influx of reports from the Internet Crime Complaint Center (IC3) about a pattern of identity theft. These complaints consistently referenced a set amount of money being taken from each bank account when there was no activity by the designated account owners and each victim being delivered credit card applications that they never signed up for.
6. On January 19, an investigation was initiated by the FBI to find the whereabouts of the cybercriminal or cybercriminals who were responsible for these complaints. Before drafting and submitting a request for a court-ordered subpoena, the logs within the IC3 complaints included the specific timestamps and IP addresses used in the logins. Utilizing internal tracing tools, each of the IP addresses connected back to a single residential broadband block that was maintained by an Internet Service Provider (ISP), and this was further verified to learn of the entire IP address range by January 23, 2025.
7. On January 26, 2025, the FBI submitted a court-authorized subpoena to request subscriber information to the ISP about the IP address used to gain access to three of the victim's accounts from January 20 to January 24, 2025.
8. On February 5, the ISP responded to the subpoena and confirmed that the IP address was assigned to LEON GILL at 4045 Allison Avenue during the times of the theft in question.
9. Between February 6 and February 9, 2025, additional subpoenas were issued to two financial institutions that were affected during this time due to the unauthorized logins. The subpoenas requested login history, device data, and account activity logs.
10. Between February 14 and February 18, 2025, responses from the financial institutions were received, showing that multiple logins to the victims' customer accounts also originated from the same IP address of LEON GILL's residence.
11. On February 18, 2025, during voluntary interviews, two of the victims provided sworn statements to validate the accuracy of their data and dates of received credit card applications on February 2 and February 5, 2025, respectively.
12. From February 18 to March 2, investigators conducted a digital forensic analysis using the metadata from the ISP and financial institution logs. The investigators found that inconsistencies appeared with the geolocation data and use of masked device identifiers, suggesting the use of a Virtual Private Network (VPN) service or other masking tools. These tools can change digital traffic to move through remote

servers, making someone appear in a different location from where they are in reality.

13. From March 3 to March 17, 2025, a team of agents conducted daily physical surveillance to watch LEON GILL's schedule. LEON GILL was seen exiting his home every morning between 8:00 AM and 9:00 AM and returning between 5:30 and 6:30 PM, reflecting an average job schedule. Due to his work schedule, agents conducted nighttime surveillance to observe potential after-hours activity related to the crimes. This was later proven with seven evenings between 12:00 AM and 3:00 AM when agents observed LEON GILL's residence and noticed the illumination of multiple screen lights in a second-floor room, suspected of being a home office.
14. On March 3, using open-source intelligence (OSINT), further evidence is shown on a deleted post from LEON GILL's public X (formerly Twitter) account @LeonGill32. In this post, it read: "Some people can't see the value in what they make available. #DigitalFootprints". While the quote could seem like it was spreading awareness about security, there is also the possibility that it is a form of gloating that lines up with the concurrent incidents of identity theft. This post indicates a familiarity with, and potentially a dismissive attitude towards, exploiting unsecured personal data, showing consistency with the nature of identity theft. The post was also deleted the following day and required using a social media scraping tool to recover the data, which raises further suspicion.
15. On March 5, a voluntary interview with victim ELISE REED confirmed that there was an incident of unauthorized access to her bank account on March 2, 2025. The logs from her bank showed that the access was from an IP address that was four miles from LEON GILL's residence. She wrote in her sworn statement that she had never been to the said area in her life and that she never authorized the access of anyone else to do anything with her account. This incident also strongly correlates with the deleted X post from March 4, 2025.
16. On March 6, 2025, the FBI retrieved public utility records and conducted a search of the ownership and rental history for the address. Based on the patterns for electricity and water, trash records confirming one individual was registered to the property supports the conclusion that LEON GILL is the only occupant of the residence. Searching through public property records and leasing documents further confirmed that LEON GILL was the only tenant.
17. On March 8, 11, and 15, LEON GILL was seen by agents entering and exiting his residence carrying a slim black laptop bag during his average schedule. This observation strongly suggests that he is transporting devices that contain evidence of illegal activity which is further corroborated by the occurrence of these three days

in these two weeks. Another theory suggests that he is attempting to transport evidence as a way to avoid detection from law enforcement.

18. On March 12, at approximately 7:00 PM, LEON GILL was observed sitting on a lawn chair while having a video call on his smartphone. The surveying agents were across the street in an unmarked vehicle with tinted windows, could casually hear certain parts of the conversation, and were situated lawfully in a public location without the use of audio enhancement equipment. The pieces from the conversation that was of note included mentioning "network drops" and needing to "reset the proxy" to "keep things running to make the goal by the weekend." The mention of a proxy also strongly confirms the possibility of VPN usage from the digital forensic analysis.
19. Between March 8 and March 14, 2025, agents were also conducting a lawful metadata analysis from publicly available breach databases and dark web market listings. Multiple identities from the IC3 reports in the past three months, including names, SSNs, and bank account information, were put up for sale on a known identity trafficking forum. Additional payment records connected to the listings showed transactions to a Bitcoin wallet address. Utilizing blockchain tracing tools, the wallet was linked to a VPN service subscription that LEON GILL previously paid for using a fake name and an email address that traced back to his X handle. This confirms the suspicions of VPN usage and his role in unauthorized access activity and the trafficking of PII.

CONCLUSION

20. Based on the foregoing facts and evidence, I believe that there is probable cause for the violation of 18 U.S.C. § § 1028, 1028A, and 1030(a)(2)(A) of the Computer Fraud and Abuse Act that will be found within Leon Gill's residence. The devices at said residence to have a high likelihood of relevant digital evidence include, but are not limited to computers, laptops, smartphones, and external storage devices such as hard drives.
21. I respectfully request that the Court issue a search and seizure warrant to authorize the examination and removal of digital devices and records from the residence. These items will then be subject to forensic analysis to uncover and secure evidence of unauthorized access to protected computers and identity theft.

Respectfully submitted,

Agent Eric Preston

Federal Bureau of Investigation

Cybercrime Division

Eric Preston

April 8, 2025