

Feb 10, 2026

s/ MMK

**Deputy Clerk, U.S. District Court
Eastern District of Wisconsin**

UNITED STATES DISTRICT COURT
for the
Eastern District of Wisconsin

United States of America)
v.)
YONG FENG WU) Case No. 26-MJ-25
(DOB: 12/18/1995))
)
)
)

Defendant(s)

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 02/02/2026 - present in the county of Milwaukee in the
Eastern District of Wisconsin, the defendant(s) violated:

Code Section

Offense Description

This criminal complaint is based on these facts:

Please see Affidavit.

Continued on the attached sheet.

Harleen Kaur

Complainant's signature

Harleen Kaur, Special Agent, DHS-HSI

Printed name and title

Sworn via telephone; transmitted via email pursuant to Fed. R. Crim. 4.1

Date: 02/10/2026

William E. Duffin
Judge's signature

Judge's signature

City and state: Milwaukee, Wisconsin

Honorable William E. Duffin, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Harleen Kaur, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that JIA DI LI and YONG FENG WU have violated Title 18, United States Code, Sections 1349 and 1956(h), conspiracy to commit wire fraud and conspiracy to launder monetary instruments, and others, known and unknown.

2. I am presently employed as a Special Agent with the Department of Homeland Security, Homeland Security Investigations (HSI), assigned to the Resident Agent in Charge Office in Milwaukee, Wisconsin, where I have been assigned to investigate crimes concerning financial crimes involved elder abuse, telemarketer scams, impersonation of public official scams, etc. I have served as a federal agent as a Special Agent with HSI since September 11, 2022. Prior to that, I was employed with Immigration and Customs Enforcement from May 2017 to September 2022. Prior to that, I was employed with United States Citizenship and Immigration Services from January 2013 until May 2017.

3. During my tenure as a Special Agent, I have completed approximately more than 800 hours of instruction at the Federal Law Enforcement Training Center in Glynco, Georgia (FLETC); of which the curriculum consisted of financial fraud, narcotics, human trafficking, illegal arms export, child exploitation, etc. Prior to my tenure as a Special Agent, I have worked as a Deportation Officer, responsible for investigating criminal and administration immigration violations of Title 8 USC statutes. Prior to my career as a Deportation Officer, I worked in the capacity of an Immigration Adjudications Officer with Fraud Detention and National Security. My work experience consisted of conducting administrative and criminal investigations that involved

marriage fraud, business fraud, and various types of fraud under Title 8 of the Immigration and Nationality Act.

4. This affidavit is being submitted in support of an application for an arrest warrant for JIA DI LI and YONG FENG WU. There is probable cause to believe that JIA DI LI and YONG FENG WU violated Title 18, United States Code §§ 1349 & 1956(h), conspiracy to commit wire fraud and conspiracy to launder monetary instruments.

5. The information contained within this affidavit is based on my personal knowledge, training and experience, as well as information provided me by other law enforcement officers assisting with this investigation. I have not included every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause for the arrest of JIA DI LI and YONG FENG WU.

PROBABLE CAUSE

Background

6. The Department of Homeland Security, Homeland Security Investigations (HSI), is investigating a government impersonation scam in which call centers located overseas impersonate DHS, SSA, FTC, and Treasury Department employees to extort money from victims under the pretense that the money would be kept safe by federal agents. The victim is contacted by or induced to contact the purported agent, on the materially false representation that the victim's personal information has been hacked or compromised. The fraudster then refers the victim to a co-conspirator posing as a law enforcement agent who directs the victim to move the victim's funds, usually in the form of cash or physical gold, to a third-party or government account for safe keeping. The co-conspirator then coordinates the transfer of the victim's funds to other scam participants who act as fake federal agents and who travel to the victim's residence to

pick up the proceeds of the wire fraud. After retrieving the proceeds from the victims in various states, the pseudo federal agents transported the proceeds to other co-conspirators through hand-to-hand transactions, electronic wire transfers, and through the mail or private freight carriers such as FedEx.

This Investigation

7. T.B. (“Victim 1”) is 70 years old and a resident of Milwaukee, Wisconsin.

8. Approximately on February 2, 2026, Victim 1 was browsing the internet on an electronic device and received a pop-up message stating their device was hacked and to call a telephone number for support. Victim 1 called the telephone number for support.

9. Victim 1 received a telephone call from an individual purporting himself to be a federal agent, Mark GRAY with the Federal Trade Commission of the U.S. Government. GRAY advised Victim 1 that his identity had been used in the commission of crimes to include money laundering, wire fraud, and child pornography.

10. To safeguard Victim 1’s money, GRAY instructed Victim 1 that they must transfer Victim 1’s money to a secure locker with the U.S. Government in Washington, D.C. GRAY instructed Victim 1 to withdraw funds from Victim 1’s multiple bank accounts and to transfer funds to two separate bank accounts.

11. On or around February 2, 2026, Victim 1 initiated a wire transfer from his Wells Fargo Bank Account, ending in 0627, and transferred \$4,500.00 to an “Alva MARINO” at 14890 Lee Dr, Denham Springs, LA, 70726, to a Wells Fargo Bank account 7946437293.

12. On the same day, Victim 1 initiated an additional wire transfer from his Educators Credit Union bank account ending in 1586 for the amount of \$35,000 to a Wells Fargo Bank

Account for a “DALAYNA LASER 325 STATE ROUTE 603 W, SHILOH, OH 44878 account number 3397285853”.

13. On February 6, 2026, GRAY instructed Victim 1 to conduct another wire transfer from his Educators Credit Union for an additional \$26,000. GRAY instructed Victim 1 to transfer \$26,000 to a “Nathaniel RICHARDSON at 2214 Tangelo St, Mission, TX 78572, a Wells Fargo Bank account number 1587567882.” Victim 1’s bank refused to transfer the money and advised Victim 1 that he was a victim of a scam.

14. On the same day, due to the bank declining to transfer funds, GRAY instructed Victim 1 to buy gold bars worth \$148,000 for safeguarding. Victim 1 went to a gold store in Milwaukee, WI to purchase gold bars. GRAY advised Victim 1 that a federal agent from FTC would come to his house to pick up the gold bars for safekeeping.

15. On February 6, 2026, Homeland Security Investigations (HSI) Resident-in-Charge (RAC) Milwaukee was contacted regarding Victim 1. HSI Milwaukee made contact with the victim at the gold store and confirmed that the victim was actively being defrauded and the scammer, “Mark GRAY” who was purporting to be a federal agent was in relation with a nationwide Microsoft scam.

16. On February 8, 2026, at the direction of HSI, a fabricated photograph was produced showing \$148,000 of gold and sent to GRAY at the phone number, 206-569-8674. Special Agents also observed additional text messages from Victim 1 and GRAY in which GRAY was asking about wire transfers. Special Agents also observed an email sent to Victim 1 from mark.gray.ftc@mail.com on February 2, 2026, in which GRAY claimed that Victim 1 was under identity theft investigation, case ID FTCDX584574, and to comply with this investigation.

17. On February 9, 2026, with cooperation of Victim 1, HSI Agents and Victim 1 recorded phone calls between GRAY and Victim 1. HSI Agents observed GRAY being insistent that the gold bars be handed to a federal agent that same day. Agents observed GRAY's tone and vocabulary to be attempting to mimic a law enforcement official, saying things such as, "your wages will be garnished, Mr. Brown", "you are fighting the government" and "the government will seize your assets and issue an arrest warrant."

18. During these recorded phone calls, GRAY advised that a federal agent will be coming to Victim 1's residence on February 10, 2026, at approximately 8:30 a.m., to pick up the gold bars.

19. On February 10, 2026, HSI Special Agents, in conjunction with local law enforcement, conducted an operation at Victim 1's residence, utilizing a package full of sham gold bars and a GPS tracking device concealed within the package. At approximately 9:00 a.m., HSI Special Agents observed an Asian male, later identified as JIA DI LI (LI), wearing black sweatpants, black hooded sweatshirt and sunglasses, walk around the block of Victim 1's residence. HSI Special Agents observed LI conversing on the phone as he circled the block. Contemporaneously, HSI Special Agents inside the residence with Victim 1 reported that GRAY was talking on the phone with Victim 1 and had instructed Victim 1 to step outside with the box of gold bars.

20. HSI Special Agents then observed Victim 1 exit the residence and stand on the front porch. Shortly thereafter, HSI Special Agents observed LI walk down the sidewalk, stop in front of Victim 1's residence, and engage in conversation with Victim 1. HSI Special Agents observed and photographed Victim 1 walk up to LI and hand over the box of gold bars to LI.

21. Upon taking possession of the package, HSI Special Agents observed LI walk approximately four blocks away from Victim 1's residence and enter the passenger side of a blue Volkswagen Taos bearing Illinois license plate FN 52487 (VEHICLE 1). HSI Special Agents observed a driver already occupying the vehicle, later identified as YONG FENG WU (WU).

22. As VEHICLE 1 left the area, HSI Special Agents conducted physical and electronic surveillance of VEHICLE 1 and the package respectively. From Victim 1's residence, VEHICLE 1 drove to the FedEx store located at 8807 Sura Ln, #107, Greenfield, WI 53228.

23. Once parked, HSI Special Agents observed LI open the package and pull out the bubble wrap in which the gold bars were encased while WU was speaking on the phone. HSI Special Agents observed LI enter the FedEx and come back out to the vehicle after a few minutes. Approximately fifteen minutes later, WU exited the vehicle and walked into the FedEx. After approximately 1-2 minutes, HSI Special Agents observed WU dash out of the Fed-Ex and run towards VEHICLE 1.

24. Based on WU's behavior, HSI Special Agents believed it probable that the operation had been compromised and WU and LI were attempting to flee. In an effort to minimize the risk of engaging in a vehicle pursuit which would increase the likelihood of escape, and out of an abundance of caution to the public and officer safety, HSI Special Agents activated their emergency lights and sirens and surrounded VEHILCE 1 as WU was arriving at the driver side door. HSI Special Agents, wearing body armor which prominently displayed badges and patches with the word "POLICE", identified themselves as police and informed LI and WU they were under arrest. LI and WU were then taken into custody without incident.

Arrest and Questioning of Both Suspects

25. During the search incident to arrest, HSI Special Agents discovered WU possessed a Virginia driver's license (DL#A69896407) bearing the name YONG FENG WU with a photo bearing the same likeness and appearance of WU.

26. During the search incident to arrest, HSI Special Agents discovered LI possessed a California driver's license (DL#F2870626) bearing the name JAI DI LI with a photo bearing the same likeness and appearance of LI.

27. Both subjects were transported to Greenfield, PD for processing. Post Miranda, WU stated that he flew from LAX to Dallas to Midway Airport in Chicago. WU was instructed to do this by a man he knew only as "Minh." WU met Minh at a party in Los Angeles approximately six (6) months ago. WU disclosed that around that time, he helped translate a conversation between Minh and an unknown black male in which the two discussed creating fake and fraudulent bank accounts for the purpose of wiring money.

28. During his trip to Milwaukee, WU stayed at a Days Inn in Milwaukee, WI per Minh's instructions. Also per Minh's instructions, WU said that yesterday he purchased a safe from Wal Mart that looked like a dictionary. Minh provided WU the victim's address and he provided WU the time to arrive at Victim 1's address.

29. Per Minh's instructions, WU stayed in the vehicle about a block away from Victim 1's house while LI walked to Victim 1's house. After retrieving the money from the victim, WU was instructed by Minh to put the gold bars into the safe that appears to be a dictionary, and FedEx the package to an unknown address. For his efforts, WU was to be paid \$200 cash plus expenses.

30. Also during the interview of WU, he revealed that he uses two phones—one for his personal use, and second phone that he uses for these pickups. To communicate with Minh, WU was instructed to use Telegram. I know from my experience that Telegram is a secure, encrypted electronic messaging platform that allows users to edit and even delete messages after they have been delivered.

31. WU also consented to a search of his phone. In the phone that WU was given for purposes of conducting the gold pickup with Victim 1, agents observed pictures and electronic messages between WU and Minh. The pictures included the box containing the gold bars from Victim 1, pictures of gold bars unwrapped. There were also pictures of gold bars being laid out on the seat of the vehicle WU was driving.

32. Post Miranda, LI stated that he met “Feng” (WU) on a Chinese social media application called “Redbook” this past January. Last Wednesday, February 4, 2026, he received a call from an unknown phone number and unknown caller stating that he (LI) could make cash to fly to Milwaukee and pick up a package. On Saturday, February 7, 2026, LI stated that he flew into Milwaukee. He stated that WU paid for the flight, and he took a separate flight from WU. LI said he first met WU at the airport. After booking a private vehicle rental through Turo, LI and WU stayed at a Days Inn.

33. The unknown male LI spoke with earlier called and told LI to wait for the order. The unknown male then called this morning and provided the address for the package pickup.

34. The unknown caller also told LI that he could make additional money if he picked up another package. LI stated that he was being paid \$200 per day while in Milwaukee and would receive another \$500 for delivering the package to FedEx. LI was supposed to be paid in Bitcoin. The unknown Male told LI he could make more money if he performed another pickup.

35. LI also provided consent to search his cell phone. All of the text messages in LI's phone are in the Chinese language. LI's phone also contained a picture of the fake gold bars that he picked up from Victim 1. LI's phone contained a screenshot of a flight itinerary from LAX to Las Vegas, Nevada, and Las Vegas, Nevada to Chicago O'Hare Airport on February 8, 2026. There were no images of an itinerary showing a flight to MKE.

CONCLUSION

36. Based on the above information, there is probable cause to believe that JIA DI LI, YONG FENG WU, and others unknown violated Title 18, United States Code, Section 1349 (conspiracy to commit wire fraud) and Section 1956(h) (conspiracy to launder monetary instruments).