

Nail Salon Worker Held Over 13 Remote IT Worker Jobs At The Same Time

A Maryland nail technician with limited computer skills used his American citizenship to front a North Korean hacker, allowing unauthorized foreign access to sensitive U.S. government aviation systems while collecting over \$970,000 for work he never performed.

Minh Phuong Vong, a nail salon technician from Bowie, Maryland, pled guilty to a scheme that allowed a foreign hacker to infiltrate sensitive FAA systems while he continued working as a nail technician at Allure Nail Spa in Bowie.

According to court documents, Vong allowed a North Korean national to use his identity to get remote software development positions with U.S. government contractors.

While Vong physically appeared for identification verification and picked up security credentials, his co-conspirator actually performed the work from overseas.



A Nail Technician That Worked On FAA Systems? Not Quite

The scheme, which ran from January to August 2023, centered around a software development position at a Virginia-based company referred to as "Company 1" in court documents.

This contractor provided software development services to various U.S. government entities, including the Federal Aviation Administration (FAA).

Since the position required U.S. citizenship and security clearance eligibility. Vong, a naturalized U.S. citizen originally from Vietnam, provided his identification but had neither the education nor skills represented on the fraudulent resume submitted to the company.



Figure 2: Screenshot of VONG taken by US Company 1 during I-9 verification process.

Instead, an individual known only as "John Doe" or "William James," who appears to have been operating from Shenyang, China, conducted the technical interviews and performed the actual software development work.

From Nail Technician to IT Impostor Making Hundreds and Thousands of Dollars

While continuing his day job at Allure Nail Spa, located at 15485 Annapolis Rd #220 in Bowie, Vong's financial situation changed dramatically.

Court records show that in 2021, he earned about \$45,000, primarily from his work at the nail salon.

However, while still working at the salon, Vong's reported income jumped to around \$430,000 in 2022 and at least \$380,000 in 2023, with most of this income coming from other employers.

80% of Salary Sent Overseas But He Paid Taxes Of All Things

Court records reveal that Vong received over \$25,000 in gross wages for work he never performed.

According to his plea agreement, Vong initially kept only 20% of the payments, transferring the remainder to overseas accounts. When this proved insufficient to cover his tax obligations, he negotiated to keep 30%.

The conspirators maintained a complex financial network, using money transfer services to move funds from Vong's U.S. bank accounts to overseas accounts held under different names.

Between June and July 2023 alone, Vong authorized the direct deposit of more than \$7,000 into an account that was then used to transfer money internationally.

His Deception Was Uncovered After His Multiple Jobs Were Discovered

The scheme began to unravel when Company 1 discovered discrepancies while processing Vong for a security clearance. T

The company learned that another firm already had "clearance ownership" of Vong in the system, suggesting he was employed elsewhere, which led to his termination in July 2023.

FBI analysis of Vong's company-issued laptop revealed it had been remotely accessed from China and Russia using software that wasn't authorized for company work. IP addresses originating from Shenyang, China were used to access U.S. government systems using Vong's credentials.

“John Doe” Was A North Korean Hacker

Evidence in court documents suggests John Doe was a North Korean national who corresponded with Vong via Skype and other messaging platforms.

Investigators found evidence that the account associated with "William James" frequently accessed North Korean websites, including the state airline Air Koryo, and made reference to visiting Pyongyang.

Nail Tech Collected \$970,000 For Work He Never Performed

As part of his guilty plea, Vong admitted that between 2021 and 2024, he used fraudulent misrepresentations to obtain employment with at least 13 different U.S. companies, who collectively paid him more than \$970,000 in salary for software development services that were actually performed by his overseas conspirators.

Vong faces a maximum sentence of 20 years in federal prison when sentenced on August 28, 2024. As part of his plea agreement, he will forfeit at least \$28,324.33, representing the proceeds from the fraudulent scheme.

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, **Aaron Zentner**, being duly sworn, depose and state as follows:

1. This Affidavit is being submitted in support of a Criminal Complaint charging **MINH PHUONG VONG** (“**VONG**”) and **JOHN DOE** charging them with conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349.

PROBABLE CAUSE

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed since 2022. I am currently assigned to the to the FBI’s Baltimore Field Office where I work a variety of national security investigations involving counterintelligence, export violations, counter-proliferation, and the violation of US sanctions. I have received extensive investigative training at the FBI’s Basic Field Training Course at Quantico, Virginia (VA). Prior to becoming a Special Agent (SA), I was an active-duty Army Officer for over nine years. As an officer I was assigned as an Investigating Officer for multiple Uniform Code of Military Justice (UCMJ) investigations regarding Army Soldiers and violations of the UCMJ. My primary military occupational specialty was as an all-source analyst. As such, my training and duties revolved around analyzing raw intelligence for military commanders to make decisions related to tactical operations and training. I continue to serve as a Major in the United States Army Reserve.

3. **VONG** is a native of Vietnam and has been a naturalized United States citizen since in or around 2000.

4. One or more unknown individuals are users of Skype account live:william.james1995 and user of email accounts minh.developer2000@gmail.com, wuhong822@outlook.com, and william.james1995@hotmail.com. There is probable cause to believe that at least one user of the

accounts, hereinafter referred to as **JOHN DOE**, a/k/a “William James” is a native of North Korea as set forth more fully in paragraphs 34 through 37.

5. US Company 1, located in Virginia, is engaged in the business of software development, including providing software development services to United States Government Entity 1. As part of the company’s work with the US Government, it develops software in support of an application which monitors aviation assets in flight in the United States. This application is used by various US government entities such as the Department of Defense, Department of Homeland Security, and Secret Service, to coordinate aviation assets.

6. US Company 2, located in Virginia, is a technology firm that advertises itself as providing services to solve complex issues for the US Government.

7. United States Government Entity 1 (“USG Entity 1”) is a federal agency headquartered in Washington D.C. Among other things, USG Entity 1 manages and disseminates sensitive information regarding US national defense matters to other federal agencies as part of its national defense program.

Vong’s Employment at US Company 1

8. In or around early 2023, US Company 1 was looking to hire a Full Stack Web Application Developer for a position supporting USG Entity 1’s national defense program. To qualify for the position, an applicant had to be a United States citizen and have the ability to obtain and maintain a security clearance at the “Secret” level.

9. On or about January 30, 2023, a Virginia-based recruiting company submitted to US Company 1 a resume for **VONG** for consideration for that position. According to the resume, **VONG** earned a Bachelor of Science degree from the University of Hawaii between 2001 to 2005, and he had 16 years of experience in the field of software development. The resume

further indicated that **VONG** had worked with USG Entity 4 from September 2021 to January 2022, and that “I had to do security clearance for this project since I had to access classified government information.”

10. In or around February 2023, the Senior Developer for US Company 1 conducted an online interview of an individual who represented that he was **VONG** for the job position. The Senior Developer took a screen shot of the individual during the interview and recommended that he be hired.



*Figure 1: Photo taken by US Company 1 of the individual who attended the **VONG** technical interview.*

11. On or about March 23, 2023, USG Entity 1 determined **VONG** met all investigative requirements for his position and had been granted a Final Suitability determination. This meant **VONG** could begin work for USG Entity 1 via the contract staffed by US Company 1.

12. On or about March 28, 2023, the Chief Executive Officer (CEO) of US Company 1 conducted a video call with **VONG** as the final step in the hiring process. During the call, **VONG** displayed his US Passport and Maryland Driver's license to verify his identity. US

Company 1 used this information to complete an I-9 form.¹ The CEO also took a screenshot of **VONG** during the video call, as set forth below.



*Figure 2: Screenshot of **VONG** taken by US Company 1 during I-9 verification process.*

13. Following the video call, US Company 1 officially hired **VONG** as a software developer and assigned him to work on a USG Entity 1 application which monitored aviation assets while in flight within the United States.

14. In or around April 2023, US Company 1 shipped **VONG** a Macbook Pro laptop that he was to use in connection with his employment. Because **VONG** was a software developer, US Company 1 gave him administrative rights for the laptop so that he could download software.

15. On or about April 11, 2023, USG Entity 1 authorized **VONG** to receive a Personal Identity Verification (“PIV”) Card. In addition to serving as a form of government identification, Federal employees and contractors use PIV cards to access facilities and systems. **VONG** physically picked up his PIV card at USG Entity 1’s headquarters, located in Washington DC, on the same day of authorization. See below for a redacted image of **VONG**’s PIV card.

¹ US employers are required to complete an I-9 form for every employee they hire.



Figure 3: PIV card assigned to **VONG** by USG Entity 1

Vong's Access to USG Entity 1 Networks and Systems

16. As indicated above at paragraph 13, **VONG** was hired by US Company 1 to work on a government contract, which was part of USG Entity 1's national defense program, to develop software used by various government entities that would allow them to coordinate aviation assets effectively. According to the USG Entity 1 Program Manager ("PM") who oversaw that program, developers assigned to the program used a project management software product called Jira to organize software development activities. For example, developers would log into Jira, get assigned a ticket of work, and then work the ticket until completing the coding assignment.

17. The PM advised that the developers working on the contract participated in a Zoom meeting on a daily basis to discuss their progress and upcoming tasks; however, they did not require participants of these meetings to have their cameras on. The PM indicated that he never actually saw **VONG**, but did hear the person who identified himself as **VONG** speak during those meetings. In particular, **VONG** would inform the group of: (1) what he did yesterday, (2)

what he planned to do that day, and (3) if there were any roadblocks in his way. **VONG** would reference specific tickets and requirements that he had worked on or planned to work on.

18. The information for the specific tickets could only be found on the .gov Jira website (USG1 Jira) used by USG Entity 1. The USG1 Jira website was not publicly available on the internet or otherwise. In order to access the site, an individual had to log into the internal USG Entity 1 Network or log into the USG1 Virtual Private Network (VPN) using unique credentials assigned to the individual by USG Entity 1. USG Entity 1's standard security procedure required a user to initially make a connection request to access the USG VPN, followed by a multifactor authentication ("MFA") prompt typically sent to the employee's cellular device or email address.

19. The USG1 VPN was located in New Jersey at a USG Entity 1 Technical Center.

20. The USG1 VPN allowed an authorized user, such as **VONG**, to establish a secure connection that was not public to others. Both the USG1 VPN and USG1 Jira website are US Government computer systems and/or networks.

21. USG Entity 1 assigned **VONG** specific credentials which allowed him to use the USG1 VPN and access the USG1 Jira website. Credentials are only assigned to those who need access.

22. After US Company 1 hired **VONG**, it submitted **VONG**'s information to the Defense Counterintelligence and Security Agency for a Secret clearance. US Company 1 subsequently learned that US Company 2 already had clearance ownership of **VONG** in the system. This meant that someone else had sponsored **VONG** for a security clearance, and therefore, that it was likely **VONG** had another employer. Concerned about the possibility that **VONG** was working another federal job, US Company 1 fired **VONG** on or about July 14, 2023.

23. According to USG Entity 1 records, **VONG** had access to USG Entity 1 networks and systems from on or about March 29, 2023, until on or about July 14, 2023. I have reviewed data

logs of **VONG**'s account for that time period. The logs reflected that the user of the account utilized multiple, and at times conflicting, IP addresses to make device access requests to connect to USG Entity 1 networks and complete the required MFA from a second device which had a device name of **VONG**'s known telephone number. For example, on March 29, 2023, the day after US Company 1 hired **VONG**, the **VONG** user account connected to the USG Entity 1 network or system multiple times with an MFA IP address located in Shenyang, Liaoning, China.

24. US Company 1 also assigned **VONG** a Slack² account to use for communicating with others within the company. According to Slack access logs provided by US Company 1, **VONG**'s account had numerous logins during the course of his employment which originated from four different IP addresses located in Shenyang, Liaoning Province, China. This is the same geographic location used to access the USG Entity 1 network and system utilizing the MFA IP address as described in the preceding paragraph.

Vong is Not The Same Individual Who Performed Work for US Company 1

25. After **VONG** was terminated, the CEO of US Company 1 showed pictures of **VONG** to the Senior Developer. The Senior Developer informed the CEO that **VONG** was not the same individual that he had interviewed online in February 2023, nor was he the individual who had participated in the company's daily virtual meetings, which were on camera, and/or performed the development work for USG Entity 1; rather, an Unknown Subject (JOHN DOE), depicted below, was the individual who engaged in all these activities. The Senior Developer never

² Slack is a cloud-based team communication platform developed by Slack Technologies that is used primarily by businesses.

interacted with the individual who partook in the March 28, 2023, video call with the CEO, also depicted below.



UNSUB during February 2023 Interview



Vong during March 2023 Interview

Figure 4: Comparison of **VONG** and the **JOHN DOE**.

26. In the course of the investigation, law enforcement also identified a LinkedIn account³ (www.linkedin.com/in/minh-phuong-VONG-9b63261ba) with the profile name of “Minh Phuong **VONG**” and the location of Bowie, Maryland. The profile indicated that **VONG** had worked for USG Entity 4, developing its “bond management system,” between in or around October 2021 to April 2023. This description is similar to the type of work listed in the **VONG** resume that was submitted to US Company 1. The profile further indicated that **VONG** worked for US Company 3, from in or around October 2021 to April 2023, and that he had worked on the development of an internal management tool for USG Entity 5.

³ According to records provided by LinkedIn, minh.developer2000@gmail.com and the URL of www.linkedin.com/in/minh-phuong-vong-9b63261ba (see Figure 7) were associated with the same LinkedIn account. The account was registered on or about October 20, 2020.

27. I submit that the person in the LinkedIn profile photograph, set forth below, is not the same person that the CEO of US Company 1 interviewed on March 28, 2023, and instead, appears to be the same or very similar to the person who participated as **VONG** in the virtual meetings at US Company 1, as depicted in paragraph 10.



*Figure 5: Profile photograph of **VONG** LinkedIn account.*

28. The investigation has further determined that the information in **VONG**'s resume, that was submitted to US Company 1, as set forth in paragraph 9 above, is contrary to the information that **VONG** provided on an Electronic Questionnaires for Investigations Processing (e-QIP) form in December 2021.⁴ On that form, **VONG** listed his education as a High School Diploma, attained in or around 2003, and attested that he did not have any additional education. **VONG** further indicated on the form that he became a software developer in September 2020, and that he had previously worked at a nail and spa business from 2011 to 2020. The form also listed

⁴ The e-QIP form is used by the US Government in conducting background investigations and reinvestigations of persons under consideration for, or retention of, public trust positions, such as the roles held by Vong. Vong affirmed on the form that he understood if he withheld, misrepresented, or falsified information on the form, he was subject to the penalties for inaccurate or false statement pursuant to 18 U.S.C. § 1001.

VONG's residence since July of 2006, as the 12315 Welling Lane, Bowie, MD 20715 and his telephone number as 240-888-3495.

Analysis of Vong's Assigned US Company 1 Laptop

29. In or around December 2023, the FBI conducted a preliminary analysis of the MacBook Pro laptop that Company 1 had assigned to **VONG**. During the review, the FBI searched for previously identified China and Russia IP addresses associated with the **VONG** Slack. The initial search resulted in the identification of log files associated with an AnyDesk application. Specifically, the files reflect that an IP address originating in Shenyang, China, used by the **VONG** Slack Account and an IP address originating in Russia, used by fullstackdeveloper917@gmail.com, were both associated with the AnyDesk Application on **VONG**'s assigned MacBook Pro laptop.

30. According to open-source research, AnyDesk supports desktop and file sharing, remote printing, and interactive access involving keyboard, mouse, and other devices. US Company 1's CEO has advised that software developers at US Company 1 should not have the AnyDesk application, or any remote software, on their laptops and that there was no need for **VONG** to use AnyDesk in connection with any of the work that he performed at US Company 1.

31. Based on my experience, training, and conversations with other law enforcement personnel, I submit there is probable cause to believe that a conspirator downloaded the AnyDesk software to **VONG**'s US Company 1 laptop in order enable **JOHN DOE**, and/or other foreign nationals, to use the laptop to secretly perform software development work and access the USG Entity 1's systems / networks in an obfuscated manner.

John Doe's Online Communications and Internet Search History

32. Records obtained from Microsoft⁵ include Skype chats between **VONG** and **JOHN DOE**. In those chats, **VONG**, as user live:.cid.be218ed6d6c0f3d9, communicated with **JOHN DOE** at live:william.james1995. Based on a review of those chats, I submit that it is reasonable to conclude that **VONG** and **JOHN DOE** coordinated efforts to ensure that **VONG**'s employer did not know that another individual or individuals in China or elsewhere were posing as **VONG** to perform work on the software development project for the USG Entity 1. For example, on approximately March 24, 2023, **VONG** and **JOHN DOE** discussed the steps that **VONG** needed to take to get the PIV card in order to work on the USG Entity 1 contract. The Skype records also contain a chat in which **VONG** shared with **JOHN DOE** photographs of himself holding up his passport and driver's license to a mirror as follows:

JOHN DOE: when can you send it to me?

VONG: Just got home

JOHN DOE: kk



VONG: Is this good? U need my id picture again?

⁵ Microsoft produced the records pursuant to a search warrant issued by United States Magistrate Judge Erin Aslan on January 10, 2024. See Case No. 1:24-mj-00051.

JOHN DOE: too close. Can u take it against mirror? And dun wear glasses.



VONG: I only got mirrir [sic] in restroom

JOHN DOE: better I think

33. My review of the Skype communications further indicates that **JOHN DOE** is a native of North Korea and a self-described software developer who claimed in a November 2020 chat that he lived in Shenyang, China. On May 10, 2023, **JOHN DOE** stated in a chat that “latest news as our foreign ministar [sic] and Chinese ambassador [sic]met.” I know from open source research that on May 9, 2023, Kyodo News, a Japanese news agency, published an article with the headline “North Korean foreign minister meets, goes fishing with new China envoy.”

34. In addition, internet history for the minh.developer2000@gmail.com account, which lists william.james1995@hotmail.com as the backup account, reflects that the account accessed repeatedly multiple websites associated with North Korea between approximately February 2023 and July 2023, including Air Koryo, which is the state-owned airline headquartered in Pyongyang, North Korea, and North Korean news media websites.

35. The Skype chats contain multiple references by **JOHN DOE** to making visits to “PY,” which I submit is a reference to Pyongyang, as well as a discussion with an unknown individual

on June 15, 2022, about visiting a specific mountain and ski resort that I know are located in North Korea.

36. Finally, in an August 20, 2022, Skype chat with the same unknown individual referenced in the paragraph above, **JOHN DOE** responded “yes,” to the question: “I heard some members in your company are working in rason [sic].” I know from open source research that Rason is a city located in the northeast part of North Korea.

Vong’s Wage Records

37. According to wage records obtained from both Virginia and Maryland, **VONG** only received wages from a single company, Allure Nail Spa LLC at Bowie (“Allure Nail Spa”), in the first three quarters of 2021. In the fourth quarter of 2021, in addition to wages from Allure Nail Spa, **VONG** received approximately \$15,000 from another US Company for a total of approximately \$45,000.

38. According to a public records database, **VONG** had a Limited Nail Technician license for Maryland and Virginia. As of December 2023, FBI surveillance personnel had observed **VONG** enter and leave the Allure Nail Spa’s location in Bowie, Maryland on multiple occasions. In addition, FBI surveillance personnel observed **VONG** using keys to unlock the front door of that business.

39. In 2022, and through quarter three of 2023, **VONG**’s source and amount of wages changed significantly. In 2022, **VONG**’s total wages increased to \$427,299. He earned only \$38,898 from Allure Nail Spa and the remainder of the reported wages were paid by multiple other employers. According to open-source research, many of those other employers were

engaged in the business of IT services and/or government contracting. This pattern continued into 2023.

Wage records by Year and Employer Source

Year	Allure Nail Spa	% of Total	Other Employers	% of Total	Total
2021	\$ 29,921	67%	\$ 14,815	33%	\$ 44,736
2022	\$ 38,898	9%	\$ 388,401	91%	\$ 427,299
2023	\$ 25,055	7%	\$ 353,712	93%	\$ 378,767
	\$ 93,874	11%	\$ 756,928	89%	\$ 850,802

**The year 2023 only includes wage record data up to Q3*

40. Based on my training, experience, and conversations with other law enforcement personnel, I submit there is probable cause to believe **VONG** did not perform the amount of work associated with the cumulative wages for more than 15 different employers, and that he instead outsourced the work and provided his credentials for protected computer systems to an unknown individual or individuals in places outside of the United States, such as China or Russia.

Financial transactions involving Vong and China

41. Payoneer Global Inc. is a financial services company that provides a global online payment processing platform. From my review of records obtained from Payoneer, as set forth below, I submit there is probable cause to believe **VONG** used the Payoneer platform to send wages that he received from US Company 1 and other employers to individuals located outside of the United States.

42. The Payoneer records reflect that the account holder ID ending in 7285 belonged to Phuong Luu Buu (“the Buu 7285 account”). The account was opened on May 8, 2018, the address on the account is in Vietnam, and the associated phone number is Vietnamese. The email

payments from a Minh Phuong **VONG**.⁶ The originators⁷ of these payments, as reflected in the Payoneer records, were listed with variations of the names of US Company 1 and other companies which, based on my review of **VONG**'s wage records, were employers of **VONG** or were a known financial processor for US Company 1.

48. The Payments data further reflects that all the payments originating in the name of **VONG** that were sent to the Buu 7285 account, which totaled \$86,849 in or around 2023, included a reference to a "GLPS Account" ending in 6801. This GLPS account number is the same as the bank account number that, according to US Company 1 records, **VONG** provided to US Company 1 for direct deposit of his salary payments.

49. According to Payoneer's "In-Network Payments," described by Payoneer as "Payouts the Customers received from or sent to other Payoneer Customers (after 2016)," between in or around December 2022 and January 2023, the Wu 4447 account sent payments totaling \$56,200 to a recipient in China with a name of Ting Yang. According to US export records, in or around January 2022, a package with cargo described as "MACK [sic] BOOK PRO" was shipped from Bowie, Maryland to China. The bill of lading for the shipper listed **VONG**'s address, name and telephone number. The bill of lading had a consignee address of 90A5 Sanhao Street, Heping District, Shenvana, China, and a contact of Ting Yang. When I conducted an open-source search

⁶ This information was located in the field titled "Account Name of Originator." According to Payoneer, the field "refers to the name under which the payment was received. This 'Account Name At Originator' column is named so, because this name of the receiver is visible on the payment initiator's side."

⁷ This information was located in the field titled 'Originator.' According to Payoneer, the field "refers to the payment initiator (the sender of the payment)."

on the consignee address, search results showed locations in Shenyang, China, which is the same region in China where IP addresses referenced in paragraph 24 above were located.

50. The Payoneer records also included an excel spreadsheet with various documents submitted by the Wu 4447 account identified as “proof” of communications with customers and copies of various invoices and contracts. Those documents included:

- A contract dated September 15, 2022, between “Minh Phuong **VONG**” as the employer and “Wu Liou” as the contractor. The contract provided that Liou, the contractor, would provide software development services to **VONG**, the employer, at an hourly rate of \$55 per hour.
- An invoice bearing the invoice number 01, an invoice date and due date of “Sep 13th, 2022,” and “IT support (implment [sic] new feature)” for a total of \$2,300. The invoices stated they were from Minh Phuong **VONG**, listed **VONG**’s residence, listed **VONG**’s known telephone number, and listed email address dreamtraveler84@yahoo.com.

According to documents provided by Yahoo Incorporated, that email is registered to a Minh Phuong **VONG** as of November 28, 2023. Both invoices were addressed to Wu Liou and listed wuhong822@outlook.com.⁸

⁸ Based on my training and experience, I know that legitimate invoices should be “from” the party providing the service and should be addressed “to” the party paying for the contracted service. As seen in the financial transactions, and as noted in the contract, the Wu 4447 account has been receiving payments for purported work performed for Vong. Therefore, the invoice should be addressed to Vong, not from Vong, if it was a legitimate invoice.

- Various screenshots of emails between the wuhong822@outlook.com and the dreamtraveler84@yahoo.com. The email messages included discussion pertaining to sending a “2300 USD” payment for “IT Support.”
- A contract, dated August 24, 2022, between US Company 4 and “Wu Liou (Minh Phuong **VONG**)” for web development services at a rate of \$65 per hour.
- A series of screenshots of what appear to be Skype conversations between **VONG** and Wu. The Skype messages included discussion on website developments and payment for development services. One of the messages from **VONG** stated: “I’m alway [sic] available on Skype,” listed the email of “dreamtravel84@yahoo.com,” and listed **VONG**’s known phone number ending in 3495. This address is nearly identical to the email address dreamtraveler84@yahoo.com.
- A Skype message from a sender with the name of “William James” that referenced “2300 [payment] to payoneer [sic].” The recovery email for minh.developer2000@gmail.com had the username of “William.james1995.”
- Wu’s response to an apparent question from Payoneer regarding his business activities in which Wu stated he was paid for the services of “programming & tech support,” that he provided services such as “mobile apps and web,” that “I work for the client, building website and mobile app for them and they pay me for that services,” and provided a URL link to a website known as Freelancer.

51. As of December 7, 2023, the website Freelancer at the URL submitted by the Wu 4447 account contained a profile with the name of “Wu L.” and a location of “Shenyang, United

States.”⁹ I submit there is probable cause to believe the listed city Shenyang is the city of Shenyang, China.

Interview of VONG

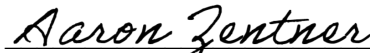
52. On May 13, 2024, I conducted a consensual non-custodial interview of **VONG** at this residence in connection with the execution of a search warrant that was issued by United States Magistrate Judge A. David Copperthite on May 9, 2024. *See* Case No. 24-mj-1157-ADC. In that interview, **VONG** claimed that in about 2020, an individual who identified himself as “William” approached him through a cell phone video game application. “William” told **VONG** that he had a way for **VONG** to make money legally. William explained to **VONG** that he should obtain webpage development jobs and then provide William with his computer access credentials. William would then perform the work, posing as **VONG**. **VONG** stated that the resume submitted in support of employment with US Company 1 was false and that he does not have a college degree or the skills to conduct the work. **VONG** stated the initial agreement was that **VONG** would get 20% of each salary payment and that the rest would go to William. **VONG** admitted that the initial 20% of each payment was not enough for the required taxes and asked William for 30%. **VONG** further admitted that he had sent one or more laptops to an address in China provided by William. When shown the picture of **JOHN DOE** (the same picture as in paragraph 10, figure 3) **VONG** identified that individual as the person know to him as William. **VONG** stated that he was not aware of any connection between William and North Korea.

CONCLUSION

⁹ This reference to the United States appears to be a typographical error, because there is no location by the name of “Shenyang” in the United States, according to open source research.

Based on the foregoing facts, I submit there is probable cause to believe that **VONG** and **JOHN DOE** conspired to commit wire fraud by making false and fraudulent statements and representations to US Company 1 over the Internet in order to convince US Company 1 to hire **VONG** as a full stack web application developer, including false statements about his education, training and job experience, for the purpose of receiving salary payments for work not performed by **VONG** in violation of 18 U.S.C. § 1349.

Date: May 15, 2024



Aaron Zentner
Special Agent
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 15th day of May, 2024.



The Honorable Adam B. Abelson
United States Magistrate Judge
District of Maryland