

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND**

**UNITED STATES OF AMERICA,**

**v.**

**MINH PHUONG NGOC VONG,**

**Defendant.**

\*  
\*  
\*  
\*  
\*  
\*  
\*

**CRIMINAL NO. DLB-24-177**

\*\*\*\*\*

**GOVERNMENT’S SENTENCING MEMORANDUM**

The Defendant, Minh Vong, pleaded guilty to a single-count indictment charging him with wire fraud conspiracy, in violation of 18 U.S.C. § 1349. Over a roughly four-year period, Mr. Vong conspired with information technology (IT) workers living in China to defraud at least thirteen U.S. companies and four U.S. government agencies into hiring Mr. Vong as a remote IT worker by lying about his credentials. In reality, Mr. Vong operated a “laptop farm,” that is, he installed remote access software on employer laptops—and shipped some employer laptops directly to China—to enable his overseas co-conspirators to perform the IT work. There is strong evidence that Mr. Vong’s co-conspirators were, in fact, working for the North Korean government. As a result of the fraudulent scheme, Mr. Vong received close to \$1 million in salary payments for IT work that he did not perform. More troublingly, Mr. Vong transmitted roughly 70-80% of the money earned to his North Korean co-conspirators and granted them access to sensitive government systems.

The government respectfully submits that a sentence of 30 months in the Bureau of Prisons, followed by 3 years of supervised release, is the sentence that best reflects the seriousness of the offense, affords adequate deterrence, protects the public, and avoids unwarranted sentencing disparities. *See* 18 U.S.C. § 3553(a).

## RELEVANT FACTS

### Background on the North Korean IT Worker Scheme

Since 2003, the Democratic Republic of Korea (North Korea) has been under sanction by the United Nations (U.N.), due to its testing and expansion of its nuclear weapons program. Since 2016, the United States has implemented comprehensive sanctions against North Korea due to the national security threats it poses, including through its nuclear weapons program. These sanctions have had the effect of cutting off North Korea from the U.S. financial system and limiting the ability of U.S. persons and companies to do business with North Korea. In recent years, North Korea's leader, Kim Jong Un, has called the United States his country's "biggest enemy" and has vowed to continue expanding North Korea's nuclear weapons program.<sup>1</sup>

North Korea has sponsored various subterfuge schemes to evade U.N. and U.S. sanctions to earn money for the regime and for its weapons programs. One such scheme involves the use of thousands of highly skilled IT workers to fraudulently obtain remote employment with companies around the world, including the U.S., using false, stolen, or borrowed identities. In order to circumvent controls put in place by U.S. companies to prevent the hiring of illicit overseas IT workers, the North Korean IT workers obtain assistance from persons residing in the United States.<sup>2</sup>

### Offense Conduct

Pursuant to his plea agreement, Mr. Vong stipulated to the following statement of facts:

Beginning at least in or about September 2020 and continuing until in or about May 2024, the defendant, Minh Phuong Ngoc **VONG**, a naturalized U.S. citizen living in Bowie, Maryland, conspired with John Doe, a/k/a "William James," a foreign national

---

<sup>1</sup> See, e.g., Kim Jong-un calls US 'biggest enemy' and says nuclear submarine plans 'complete,' *The Guardian*, Jan. 8, 2021, available at <https://www.theguardian.com/world/2021/jan/09/kim-jong-un-calls-us-biggest-enemy-and-says-nuclear-submarine-plans-complete> (last visited Nov. 21, 2025).

<sup>2</sup> See Public Service Announcement, "North Korean IT Worker Threats to U.S. Businesses," *Federal Bureau of Investigation*, Jul. 23, 2025, available at <https://www.ic3.gov/PSA/2025/PSA250723-4> (last visited Nov. 24, 2025).

living in Shenyang, China, and one or more others, to defraud various U.S. companies into hiring **VONG** as a remote software developer through materially false representations about **VONG**'s education, training, and work experience. Thereafter, Doe, posing as **VONG**, used **VONG**'s computer access credentials to perform the software development work, thereby causing the U.S. companies to transmit salary payments via interstate wire communications to **VONG**, portions of which **VONG** caused to be transmitted by wire communications to overseas bank accounts for Doe and other conspirators. **VONG** installed remote access software on his computers to facilitate Doe's access to them, which also helped conceal Doe's location in China.

For instance, on January 30, 2023, Doe caused a fraudulent resumé in **VONG**'s name to be submitted to Virginia-based technology company ("U.S. Company 1") for the position of web application developer, a position which required that the applicant be a U.S. citizen. The resumé falsely represented that **VONG** had earned a Bachelor of Science degree from the University of Hawaii and had 16 years of experience in the field of software development. On March 28, 2023, **VONG** participated in an online video job interview with the Chief Executive Officer of U.S. Company 1 in which **VONG** verified his identity and citizenship by holding up to the screen his Maryland driver's license and U.S. passport. U.S. Company 1 used this information to complete an I-9 form for **VONG** verifying his citizenship and eligibility for employment.

Following the video interview, U.S. Company 1 officially hired **VONG** as a software developer and assigned him to work on a contract for the Federal Aviation Administration (FAA) involving a particular software application. This software application was used by various U.S. government agencies to manage sensitive information regarding national defense matters. U.S. Company 1 shipped **VONG** a Macbook Pro laptop that he was to use in connection with his employment, and the FAA authorized him to receive a Personal Identity Verification ("PIV") card to access government facilities and systems. Between March 2023 and July 2023, Doe, while in China, used **VONG**'s computer access credentials to perform the software development work and participate in online meetings with U.S. Company 1 and FAA representatives, all the while pretending to be **VONG**.

Doe and **VONG** communicated via an online messaging platform about the remote software developer job at U.S. Company 1, the steps **VONG** needed to take in order to get hired for the position, and various matters that arose during the time that **VONG** was pretending to perform—and Doe was actually performing—the job at U.S. Company 1. For instance, on March 24, 2023, **VONG** and Doe (using the moniker "William James") engaged in the following conversation over the online messaging platform:

Doe:           btw bro, i need you to go and get piv card again... new job

...

**VONG**:        I [sic] for FAa piv card?

Doe:           yes

**VONG:** What company is our joba [sic]

**Doe:** [U.S. Company 1]

As a result of **VONG's** fraudulent misrepresentations, U.S. Company 1 transmitted more than \$28,000 in gross wages to **VONG** via interstate wire communications for work that **VONG** never performed. **VONG** knowingly caused portions of this money to be transmitted via wire communications to overseas bank accounts for Doe and other conspirators.

May 13, 2024 Search Warrant & Interview

On May 13, 2024, FBI agents executed a search warrant at **VONG's** residence in Bowie, Maryland. From the residence, the agents recovered the following items, among others:

- i. silver Apple Macbook Pro laptop, serial number GQDHQXP6TF;
- ii. black Dell laptop, model Latitude E7740;
- iii. iPhone 14 Pro Max, serial number CD6D7VXJYR;
- iv. gray laptop, model ANL5, serial number GD5095P23AJ927042;
- v. silver HP laptop, serial number 5CD236C9J5;
- vi. Lenova laptop, serial number R90ZDFCA;
- vii. two Canadian coins worth 200.00 Canadian dollars;
- viii. \$13,715.00 in U.S. currency;
- ix. iPhone 11 Pro Max, serial number FK1ZL2Y7N70P with blue case;
- x. iPhone 15 Pro Max serial number FGX4XLQJ6M with black case; and
- xi. iPhone 14 Pro, serial number FGHGC6CZPH.

**VONG** agreed to a voluntary interview with FBI agents. During the interview, **VONG** admitted that he met Doe via an online gaming platform and agreed to participate in the scheme to defraud U.S. companies by posing as a software developer and granting Doe his computer access credentials. **VONG** admitted that, in reality, he had no college degree or background in software development and did not perform any of the software development work for the U.S. companies with which he was employed. Instead, **VONG** allowed Doe to use **VONG's** computer access credentials in order to remotely perform software development work for the U.S. companies and U.S. government entities. **VONG** also mailed laptops to Doe in China on two occasions. **VONG** acknowledged that he knew Doe was not a U.S. citizen and was not eligible to perform the software development work for the U.S. companies or U.S. government entities. **VONG** stated that he kept between 20% and 30% of the wages earned through the scheme and transmitted the remainder to bank accounts controlled by Doe and/or other conspirators.

Victims

Between 2021 and 2024, **VONG** used fraudulent misrepresentations to obtain employment with at least 13 different United States companies, who collectively paid **VONG** a total of more than \$970,000 in salary for software development services that were, unbeknownst to them, performed by Doe and/or other overseas conspirators. The chart below shows the salaries paid to **VONG** by some of the defrauded companies during his period of employment with them:

Defrauded Company	Period of Employment	Salary Paid
U.S. Company 1	03/28/2023 – 07/14/2023	\$28,324.33
U.S. Company 2	09/28/2023 – 03/28/2024	\$44,292.36
U.S. Company 3	07/10/2023 – 07/19/2023	\$4,829.55
U.S. Company 4	10/25/2021 – 03/31/2023	\$156,203.79
U.S. Company 5	05/08/2023 – 12/29/2023	\$67,200.00
U.S. Company 6	10/31/2022 – 05/21/2024	\$170,715.34
U.S. Company 7	11/12/2020 – 01/04/2022	\$99,701.29
U.S. Company 8	03/06/2023 – 05/24/2023	\$28,086.12
U.S. Company 9	01/17/2022 – 01/05/2023	\$158,752.81
U.S. Company 10	05/22/2023 – 09/29/2023	\$43,801.43
U.S. Company 11	04/04/2022 – 06/23/2022	\$29,545.13
U.S. Company 12	02/20/2023 – 05/19/2023	\$44,588.25
U.S. Company 13	09/04/2022 - 04/01/2023	\$63,846.41
U.S. Company 14	08/08/2022 – 03/22/2023	\$37,651.52
<b>TOTAL</b>		<b>\$977,538.33</b>

Throughout the relevant time period, **VONG** worked as a nail technician at [a nail spa] in Bowie, Maryland, earning roughly \$20 per hour. According to Maryland wage records, during the first three quarters of 2021, **VONG** received wages exclusively from Allure Nail Spa, earning less than \$30,000. However, beginning in the fourth quarter of 2021 and continuing through the third quarter of 2023, **VONG** received wages from multiple other U.S. companies, and the amount of his wages increased roughly ten-fold. The chart below shows **VONG**'s wage records by year and employer source:

**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	\$ 28,827	6%	\$ 439,132	94%	\$ 467,959
2024	\$ 6,465	9%	\$ 66,813	91%	\$ 73,278
	\$ 104,111	10%	\$ 909,161	90%	\$ 1,013,272

*\*The year 2024 only includes wage record data up to Q4*

Several of the defrauded companies contracted out **VONG's** services to United States government agencies, including the [Department of Transportation's] FAA, the [Department of Commerce's] Census Bureau, the Department of Agriculture, and the Department of the Interior. As a result of **VONG's** fraudulent misrepresentations, these government agencies unknowingly granted access to sensitive government systems to Doe and other overseas conspirators, who accessed those systems from IP addresses in China.

ECF 29 (Plea Agreement), Attachment A.

Although Mr. Vong's overseas co-conspirator was living in China during the relevant time frame, there is strong evidence that he was, in fact, working for North Korea. For instance, on May 10, 2023, in a Skype chat with an unknown individual, Doe stated: "latest news as our foreign minister [sic] and Chinese ambassador met." Based on open-source research, 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."

Furthermore, Doe's Skype chats contain multiple references by Doe to making visits to "PY," which is commonly used as a reference to Pyongyang. And on June 15, 2022, there was a discussion between Doe and an unknown individual about visiting a specific mountain and ski resort located in North Korea.

In addition, in a Skype chat on August 20, 2022, the same unknown individual asked Doe, "I heard some members in your company are working in rason[?]" Rason is a city located in the northeast part of North Korea. Doe responded, "yes."

Finally, internet history for Doe's Gmail account reflects that the account was used to access multiple websites associated with North Korea between approximately February 2023 and July 2023, including the website for Air Koryo, which is the state-owned airline headquartered in Pyongyang, North Korea, as well as North Korean news media websites.

Mr. Vong has denied knowing that Doe was North Korean. But the evidence shows he knew Doe was located in Shenyang, China, near the border of North Korea. In fact, in a Skype chat with Doe on November 28, 2020, when Doe mentioned that he lived in Shenyang, China, Mr. Vong responded, “Damn . . . North Korean alliance.” He added, “Next to north korea.” Doe did not respond to these messages. Nonetheless, based on these messages, we believe Mr. Vong was at least cognizant of the possibility that Doe had a connection to North Korea.

### **ADVISORY SENTENCING GUIDELINES**

The parties agree with U.S. Probation’s calculation of Mr. Vong’s advisory sentencing guidelines. The base offense level is 7 pursuant to U.S.S.G. § 2X1.1(a), 2B1.1(a)(1) because Mr. Vong was convicted of wire fraud conspiracy in violation of 18 U.S.C. § 1349, and the offense of conviction has a statutory maximum term of imprisonment of 20 years or more. ECF 44 (PSR), at ¶ 24.

There is a 2-level upward adjustment under U.S.S.G. § 2B1.1(b)(2)(A)(i) because the offense involved 10 or more victims. *Id.*

There is a 2-level upward adjustment under U.S.S.G. § 2B1.1(b)(10)(B) because a substantial part of the fraudulent scheme was committed from outside the United States. *Id.*

The parties agree *not* to apply a 14-level upward adjustment under U.S.S.G. § 2B1.1(b)(1)(H) and Application Note 3(B), although the offense involved a loss that cannot reasonably be determined, and the offense involved a gain to the conspirators of more than \$550,000. *Id.* Instead, the parties agree that an equivalent 14-level upward adjustment is warranted pursuant to U.S.S.G. § 2B1.1 Application Note 21(A)(ii), because the offense caused or risked substantial non-monetary harm, namely, harm to the national security of the United States. *Id.* ¶ 32. The parties believe this upward departure more appropriately reflects the greatest harms

in this case, which were generating revenue supporting North Korea's weapons programs and enabling foreign malign actors to access sensitive U.S. government systems, which go beyond mere pecuniary loss.

There is a 3-level reduction under U.S.S.G. § 3E1.1(a) based on Mr. Vong's acceptance of responsibility. *Id.* ¶¶ 30, 32. The resulting offense level is 20. *Id.* ¶ 32. Mr. Vong is in criminal history category I. *Id.* ¶ 35. The advisory guidelines range based on an offense level 20 and criminal history category I is 33 to 41 months' imprisonment.

### **ANALYSIS OF FACTORS UNDER 18 U.S.C. § 3553**

The nature and circumstances of the offense are serious. The defendant defrauded at least thirteen U.S. companies and four U.S. government agencies out of close to \$1 million. He knew that his overseas co-conspirators were not authorized to work in the U.S. and that they would not be hired if the employers knew the truth. He knew that he was transmitting large sums of money to unknown individuals located in China, who may have interests adverse to the United States. He shipped two employer laptops to Shenyang, China, a city that he knew was near the border of North Korea. Although he denies knowing that his overseas co-conspirators were working for North Korea, he at least seems to have been aware of a *risk* that they were, given his comment about a "North Korean alliance." Regardless of the defendant's knowledge of North Korea's involvement in the scheme, the reality is that the proceeds of the scheme, excluding the funds that the defendant pocketed for his role (roughly \$200,000), went to individuals overseas in support of North Korea. And more troublingly still, these individuals were granted access to sensitive government systems.

The defendant has no criminal history, and he has accepted responsibility and demonstrated remorse for his crime. These factors weigh in favor of a lower sentence. However, it is important

to note that this conviction did not stem from a single, impulsive act. The defendant played an integral role in the scheme over a roughly four-year period. He took daily actions to keep the complex scheme in operation and took steps to hide the fraud from his employers. Indeed, without his assistance, Mr. Vong's co-conspirators would have been unable to obtain these jobs in the first place.

There is a strong need for general deterrence. The North Korean IT worker scheme employs thousands of highly skilled IT workers to work remotely for U.S. companies using false identities and generate revenue that is funneled back to North Korea. North Korea has exploited the COVID-19 pandemic and the advent of 100% remote work positions in the U.S., which have increased the number of U.S. jobs accessible to this and similar threat groups. Additionally, changes to hiring practices and to employment eligibility verification rules have made it easier for North Korean IT workers to obtain employment at the largest and smallest U.S. companies. A 2024 U.N. Panel of Experts report estimates that the technology sector continues to be a key moneymaker for North Korea, with an estimated 3,000 North Korean IT workers abroad and another 1,000 more operating inside North Korea, generating \$250-600 million annually, most of which is returned to the regime.<sup>3</sup>

This scheme, and others like it, would not be successful without U.S.-based facilitators like the defendant, who willingly operated a laptop farm for overseas individuals, defrauded U.S. companies and government agencies, and pocketed a substantial sum of money for his role. A sentence that is too lenient would convey the wrong message to both North Korean IT workers

---

<sup>3</sup> U.N. Security Council, Final Report of the Panel of Experts submitted pursuant to Resolution 2680 (2023), U.N. Doc. S/2024/215, at 50–51 (Mar. 7, 2024), <https://www.securitycouncilreport.org/atf/cf/%7B65BF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S%202024%20215.pdf>.

and current and future U.S.-based facilitators that this conduct is tolerated in the U.S. and worth the risk of being caught by U.S. law enforcement.

To the government's knowledge, there has been only one other case involving a North Korea IT worker scheme that has proceeded to sentencing thus far—the case of *United States v. Christina Chapman*, D.D.C. Crim. No. 24-220. In that case, the U.S.-based facilitator was sentenced to 102 months in prison. *See* Ex. 1 (*Chapman* Sentencing Transcript). It is not a perfect comparison because Chapman facilitated fraud against a larger number of employers and generated a larger sum of money that was funneled to the North Korean regime. Moreover, unlike this case, Chapman's case also involved aggravated identity theft, bank fraud, money laundering, and obstruction of justice. We seek a far lower sentence of 30 months in this case based on the specific facts and circumstances of Mr. Vong's conduct. Nonetheless, we believe much of the *Chapman* court's reasoning is applicable here. As the court there explained:

Ms. Chapman knew what she was doing was wrong. She knew that she was assisting some enemy of the United States. It is not clear which enemy she thought, but she knew it was an enemy of the United States. She may have unwittingly gotten involved at first, but she—as she continued through this process she knew what she was doing was unlawful. And ... the consequences of what she did are extremely serious. They were real live victims whose lives were affected by her conduct, companies who were affected by her conduct. And most significantly from my perspective, the North Korean government was benefitted by her conduct in a manner that was material. And whether she knew it was North Korea or not or thought it was China or Pakistan, she thought she was helping some enemy of the United States. And I do think that the national security consequences of this case and cases like it are extremely, extremely serious.

Ex. 1, at 32–33. Although the court found that Ms. Chapman was “genuinely remorseful” and “the likelihood of recidivism [was] extremely low,” the court nevertheless imposed a substantial sentence, saying: “courts are going to take this really, really seriously because the consequences to the safety of our nation are at issue here.” *Id.* at 34.

