



---

PRESS RELEASE

# Arizona Woman Sentenced for \$17M Information Technology Worker Fraud Scheme that Generated Revenue for North Korea

---

Thursday, July 24, 2025

**For Immediate Release**

Office of Public Affairs

An Arizona woman was sentenced today to 102 months in prison for her role in a fraudulent scheme that assisted North Korean Information Technology (IT) workers posing as U.S. citizens and residents with obtaining remote IT positions at more than 300 U.S. companies. The scheme generated more than \$17 million in illicit revenue for Chapman and for the Democratic People's Republic of Korea (DPRK or North Korea).

Christina Marie Chapman, 50, of Litchfield Park, Arizona, pleaded guilty on Feb. 11 in the District of Columbia to conspiracy to commit wire fraud, aggravated identity theft, and conspiracy to launder monetary instruments. In addition to the 102-month prison term, U.S. District Court Judge Randolph D. Moss ordered Chapman to serve three years of supervised release, to forfeit \$284,555.92 that was to be paid to the North Koreans, and to pay a judgment of \$176,850.

“Christina Chapman perpetrated a years’ long scheme that resulted in millions of dollars raised for the DPRK regime, exploited more than 300 American companies and government agencies, and stole dozens of identities of American citizens,” said Acting Assistant Attorney General Matthew R. Galeotti of the Justice Department’s Criminal Division. “Chapman made the wrong calculation: short term personal gains that inflict harm on our citizens and support a foreign

adversary will have severe long term consequences. I encourage companies to remain vigilant of these cyber threats, and warn individuals who may be tempted by similar schemes to take heed of today's sentence."

"North Korea is not just a threat to the homeland from afar. It is an enemy within. It is perpetrating fraud on American citizens, American companies, and American banks. It is a threat to Main Street in every sense of the word," said U.S. Attorney Jeanine Ferris Pirro for the District of Columbia. "The call is coming from inside the house. If this happened to these big banks, to these Fortune 500, brand name, quintessential American companies, it can or is happening at your company. Corporations failing to verify virtual employees pose a security risk for all. You are the first line of defense against the North Korean threat."

"The North Korean regime has generated millions of dollars for its nuclear weapons program by victimizing American citizens, businesses, and financial institutions," said Assistant Director Rozhavsky of the FBI's Counterintelligence Division. "However, even an adversary as sophisticated as the North Korean government can't succeed without the assistance of willing U.S. citizens like Christina Chapman, who was sentenced today for her role in an elaborate scheme to defraud more than 300 American companies by helping North Korean IT workers gain virtual employment and launder the money they earned. Today's sentencing demonstrates that the FBI will work tirelessly with our partners to defend the homeland and hold those accountable who aid our adversaries."

"The sentencing today demonstrates the great lengths to which the North Korean government will go in its efforts and resources to fund its illicit activities. The FBI continues to pursue these threat actors to disrupt their network and hold those accountable wherever they may be," said Special Agent in Charge Heith Janke of the FBI Phoenix Field Office.

"Today's sentencing brings justice to the victims whose identities were stolen for this international fraud scheme," said Special Agent in Charge Carissa Messick of the IRS Criminal Investigation (IRS-CI) Phoenix Field Office. "The scheme was elaborate. If this sentencing proves anything, it's that no amount of obfuscation will prevent IRS-CI and our law enforcement partners from tracking down those that wish to steal the identities of U.S. nationals, launder money, or engage in criminality that jeopardizes national security."

The case involved one of the largest North Korean IT worker fraud schemes charged by the Department of Justice, with 68 identities stolen from victims in the United States and 309 U.S. businesses and two international businesses defrauded.

According to court documents, North Korea has deployed thousands of highly skilled IT workers around the world, including to the United States, to obtain remote employment using false, stolen, or borrowed identities of U.S. persons. To circumvent controls employed by U.S.

companies to prevent the hiring of illicit overseas IT workers, the North Korean IT workers obtain assistance from U.S.-based collaborators.

Chapman helped North Korean IT workers obtain jobs at 309 U.S. companies, including Fortune 500 corporations. The impacted companies included a top-five major television network, a Silicon Valley technology company, an aerospace manufacturer, an American car maker, a luxury retail store, and a U.S. media and entertainment company. Some of the companies were targeted by the IT workers, who maintained a repository of postings for companies that they wanted to employ them. The IT workers also attempted to obtain employment at two different U.S. government agencies, although these efforts were generally unsuccessful.

Chapman operated a “laptop farm” where she received and hosted computers from the U.S. companies at her home, deceiving the companies into believing that the work was being performed in the United States. Chapman also shipped 49 laptops and other devices supplied by U.S. companies to locations overseas, including multiple shipments to a city in China on the border with North Korea. More than 90 laptops were seized from Chapman’s home following the execution of a search warrant in October 2023.



Christina Chapman organized and stored U.S. company laptops in her home, and included notes identifying the U.S. company and identity associated with each laptop.



Much of the millions of dollars in income generated by the scheme was falsely reported to the IRS and Social Security Administration in the names of actual U.S. individuals whose identities had been stolen or borrowed. Additionally, Chapman received and forged payroll checks in the names of the stolen identities used by the IT workers and received IT workers' wages through direct deposit from U.S. companies into her U.S. financial accounts. Chapman further transferred the proceeds from the scheme to individuals overseas.

This case was investigated by the FBI Phoenix Field Office, and the IRS-CI Phoenix Field Office. Assistance was provided by the FBI Chicago Field Office.

Trial Attorney Ashley R. Pungello of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Karen P. Seifert for the District of Columbia prosecuted the case, with assistance from Paralegal Specialist Jorge Casillas. Assistant U.S. Attorney Joshua Rothstein for the District of Columbia, the Victim Witness Unit, the U.S. Attorney's Office for the District of Arizona, and the National Security Division's National Security Cyber Section also provided assistance.

\*\*\*

In a coordinated effort, FBI Phoenix also issued [guidance](#) for HR professionals on detecting North Korean IT workers, and the Department of State issued guidance on the North Korean IT worker threat.

Prior guidance was issued by the FBI, State Department, and the Department of the Treasury on this threat in a [May 2022 advisory](#), and by the United States and the Republic of Korea (South Korea) in [October 2023](#). The FBI issued updated guidance in [May 2024](#) regarding the use of U.S.

persons acting as facilitators by providing a U.S.-based location for U.S. companies to send devices and a U.S.-based internet connection for access to U.S. company networks and in [January 2025](#) concerning the extortion and theft of sensitive company data by North Korean IT workers, along with recommended mitigations.

*Updated July 24, 2025*

## Components

[Criminal Division](#) | [Criminal-Computer Crime and Intellectual Property Section](#) | [Federal Bureau of Investigation \(FBI\)](#) | [USAO - District of Columbia](#)

Press Release Number: 25-785

## Related Content

---

---

### **PRESS RELEASE**

#### **Three More Minneapolis Gang Members Charged with RICO Conspiracy and Murder**

A federal grand jury in Minneapolis charged three additional alleged members or associates of the violent street gang known as the Lows, bringing the total number of defendants in this...

August 26, 2025

### **PRESS RELEASE**

#### **Gambian Man, First Non-U.S. National Convicted of Torture, Sentenced to More Than 67 Years in Prison**

Michael Sang Correa, 46, was sentenced today to 810 months in prison by Senior Judge Christine M. Arguello for the District of Colorado after being convicted of one count of...

August 22, 2025

## PRESS RELEASE

### Florida Man Sentenced to Over Six Years for Witness Retaliation Assault

A Florida man was sentenced today to six years and 10 months in prison for assaulting an individual in retaliation for testimony that the victim provided during the assailant's trial...

August 22, 2025



#### Office of Public Affairs

U.S. Department of Justice  
950 Pennsylvania Avenue, NW  
Washington DC 20530



Office of Public Affairs Direct Line  
202-514-2007

Department of Justice Main Switchboard  
202-514-2000