https://www.wsj.com/business/north-korea-remote-jobs-e4daa727

North Korea Infiltrates U.S. Remote Jobs—With the Help of Everyday Americans

A LinkedIn message drew a former waitress in Minnesota into a type of intricate scam involving illegal paychecks and stolen data

By Robert McMillan Follow *and Dustin Volz* Follow

May 27, 2025 9:00 pm ET

Christina Chapman looked the part of an everyday American trying to make a name for herself in hustle culture.

In prolific posts on her TikTok account, which grew to more than 100,000 followers, she talked about her busy life working from home with clients in the computer business and the fantasy book she had started writing. She posted about liberal political causes, her meals and her travels to see her favorite Japanese pop band.

Yet in reality the 50-year-old was the operator of a "laptop farm," filling her home with computers that allowed North Koreans to take jobs as U.S. tech workers and illegally collect $17.1 million in paychecks from more than 300 American companies, according to federal prosecutors.

In a June 2023 video, she said she didn't have time to make her own breakfast that morning—"my clients are going crazy," she said. Then she describes the açaí bowl and piña colada smoothie she bought. As she talks, at least 10 open laptops are visible on the racks behind her, their fans audibly whirring, with more off to the side.

Chapman was one of an estimated several dozen "laptop farmers" that have popped up across the U.S. as part of a scam to infiltrate American companies and earn money for cash-strapped North Korea. People like Chapman typically operate dozens of laptops meant to be used by legitimate remote workers living in the U.S.

What the employers—and often the farmers themselves—don't realize is that the workers are North Koreans living abroad but using stolen U.S. identities. Once they get a job, they coordinate with someone like Chapman who can provide some American cover—accepting deliveries of the

TAP TO WATCH

In 2023, Christina Chapman posted a TikTok that had racks of laptops visible in the background. The Wall Street Journal highlighted the laptops in this clip of the video.

computer, setting up the online connections and helping facilitate paychecks. Meanwhile the North Koreans log into the laptops from overseas every day through remote-access software.

Chapman fell into her role after she got a request on LinkedIn to "be the U.S. face" for a company that got jobs for overseas IT workers, according to court documents. There's no indication that she knew she was working with North Koreans.

The Federal Bureau of Investigation says the scam more broadly involves thousands of North Korean workers and brings hundreds of millions of dollars a year to the country. "That's a material percentage of their economy," said Gregory Austin, a section chief with the FBI.

With international sanctions freezing money flows, North Korea has grown creative in its quest for cash. North Korean hackers have stolen more than $6 billion in cryptocurrency, according to blockchain analytics firm Chainalysis. With laptop farming, they have flipped the gig economy on its head and found ingenious ways to trick companies into handing over paychecks.

It's becoming a bigger problem for companies that use remote workers, said Adam Meyers, a senior vice president at CrowdStrike. The cybersecurity company recently identified about 150 cases of North Korean workers on customer networks, and has identified laptop farms in at least eight states.

The workers, typically technology specialists, are trained in North Korea's technical education programs. Some stay in North Korea while others fan out to countries like China or Russia—to hide their North Korean connection and benefit from more reliable internet—before seeking their fortunes as IT workers for Western companies.

Sometimes they're terrible employees and are quickly dismissed. Others last for months or even years.

"These DPRK IT workers are absolutely able to hold down jobs that pay in the low six figures in U.S. companies and sometimes they can hold multiple of these jobs," the FBI's Austin said.

They work for almost any conceivable sector that uses remote labor. One cybersecurity company discovered two years ago that it had employed nine North Korean workers—all via staffing agencies, according to court documents. Two of them logged in each morning through Chapman's laptop farm.

The workers sometimes appear to steal data for espionage or to use as ransom.

Late last year, Ryan Goldberg, an incident response manager at cybersecurity company Sygnia, got a look at a laptop that was returned to a client—a life-sciences company—after the FBI raided an East Coast laptop farm.

As the MacBook booted up, he was amazed by what he saw: a series of seven custom-written programs designed to get around antivirus software and firewalls, giving the North Koreans a virtually undetectable back door into the corporate network.

One program allowed them to spy on Zoom meetings. Others could be used to download sensitive data without being detected. "The way they were employing remote control was something we'd never seen before," said Goldberg. "They really thought outside of the box on this."

But first, they need to recruit an American to open the door.

A 2024 FBI poster for North Korean nationals wanted in a scheme in which workers used false identities to get remote jobs with U.S. companies. PHOTO: JIM SALTER/AP

'I don't know what to do'

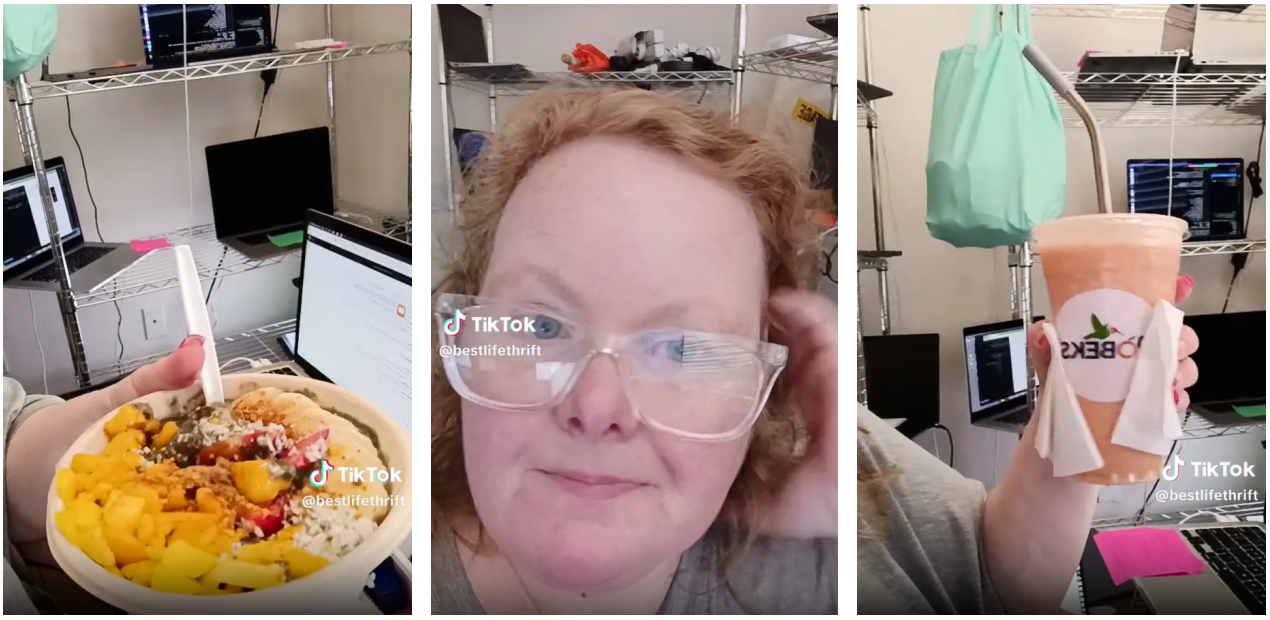
The North Koreans start by sending out thousands of requests to people on job-related sites such as LinkedIn, Upwork and Fiver, investigators say. Their wide net often catches people in a time of financial need—people like Chapman, who got the LinkedIn message in March 2020.

Chapman, a former waitress and massage therapist then living in a small town north of Minneapolis, had finished a coding boot camp around that time, hoping to become a web developer. It wasn't working out. On Jan. 21, 2021, she pleaded for help finding a place to live in a tearful post on TikTok.

"I live in a travel trailer. I don't have running water; I don't have a working bathroom. And now I don't have heat," she said. "I'm really scared. I don't know what to do."

Court documents say Chapman began working with the North Koreans by around October 2020 and her involvement steadily grew. By January 2023, she had moved to Arizona and was earning enough income to move into a four-bedroom home that she shared with a roommate in Phoenix, with a yard for her chihuahuas, including Henry, Serenity and Bearito.

Chapman was a jack-of-all-trades for her “clients.” She’d help send their falsified W-2 tax forms or other verification documents when they got hired. The workers had their company laptops sent to her address. She’d unpack them, install remote access software and power them on for the North Koreans to log on. She made sure connections ran smoothly and helped troubleshoot any issues. Sticky notes on the computers identified the company and the worker they were supposed to belong to.



Screenshots from Chapman’s June 2023 Tiktok video with laptops in the background.

In April 2022, a worker who had just been hired as an American, using the screen name “Max,” messaged Chapman about an I-9 form, used to establish an employee’s eligibility for work in the U.S.

“Please ship out the hand signed I-9 form by the end of the day,” he wrote. “The company send message again. Could you please help me today?”

“Yes. I’ll get it out today,” Chapman wrote. “I did my best to copy your signature.”

“haha. Thank you,” he replied.

The devices didn’t always stay at her house. She shipped 49 laptops, tablets and other computers overseas, many to Dandong, a Chinese city on the border with North Korea.

She sometimes received paychecks at her house, signed them and deposited them to her bank, and then forwarded the funds to another account after taking a cut, according to court documents.

AI video tricks

One of the North Koreans' most remarkable feats is the way they leverage gig workers to get around almost any controls corporations can put up to detect them.

"They realized it's really easy to hire people to do anything," said Taylor Monahan, a security researcher with the crypto company MetaMask who is part of a tightknit community of investigators that studies North Korean teleworkers. "They just know the system that well."

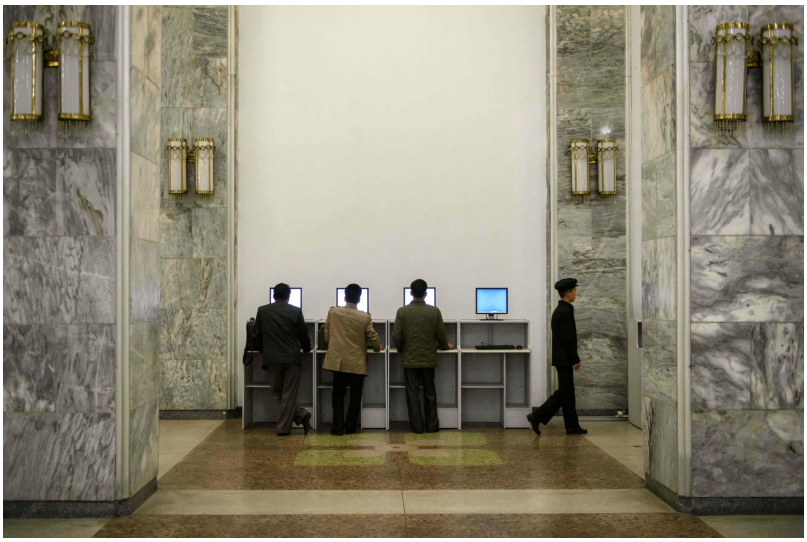
Beyond laptop farms, they hire U.S. proxies to simply provide a mailing address to receive packages or paychecks, or to hand over their own identification to the North Koreans. Others will pass "liveness checks"—pretending to be the actual employee every time the employer needs them to turn a camera on. They hire people to create legitimate accounts on freelance platforms that are then handed over to the North Koreans.

At one point, North Koreans were using generative artificial intelligence to alter their appearance during online job interviews. But when interviewers figured out an easy way to detect it—ask interviewees to wave their hand in front of their face, a move that causes the AI software to glitch—the North Koreans started hiring tech-savvy people to ace the interviews, Monahan said.

The scam also creates problems for unsuspecting Americans whose personal information gets stolen to obtain jobs, said Meyers of CrowdStrike. Typically the North Koreans take the minimum amount of tax deductions, leaving the person whose identity they stole with a tax liability, he said. Chapman's laptop farm "created false tax liabilities for more than 35 U.S. persons," prosecutors said in court documents.

For companies employing the North Koreans, their data is at risk—and the workers Chapman helped were able to get jobs at "a top-5 national television network and media company, a premier Silicon Valley technology company, an aerospace and defense manufacturer, an iconic American car manufacturer, a high-end retail chain, and one of the most recognizable media and entertainment companies in the world," according to her indictment.

Chapman helped one worker, "Marcus," set up for a remote job he'd obtained at a "classic American clothing brand headquartered in California" through an IT staffing agency. Six months into his job, Marcus was downloading data from his employer and sending it off to a computer in Nigeria.



People used computers at the Grand People's Study House in Pyongyang in 2019. PHOTO: ED JONES/AFP/GETTY IMAGES

'Computer business'

Chapman's posts on TikTok ramped up in 2023. She described her work life in one, saying she's had another busy morning. "I start at 5:30, go straight to my office, which is the next door away from my bedroom, and I start taking care of my clients. Computer business," she said. "It's now almost noon and I'm just now getting to eat."

In another post that May, she unboxed a $72 green ring in her backyard. "This is my first jewelry I've ever purchased with care instructions," she said. That night she and her roommate went out to see a drunken Shakespeare performance, where the players are inebriated.

In August she traveled to Canada and Japan to see her favorite Japanese boy band. That same month, she messaged with several overseas workers about their I-9 forms.

"In the future, I hope you guys can find other people to do your physical I9s. These are federal documents. I will SEND them for you, but have someone else do the paperwork. I can go to FEDERAL PRISON for falsifying federal documents," she wrote, according to her indictment.

The North Koreans deemed Chapman so helpful that two months later, when they grew frustrated with another alleged laptop farm operator in Virginia, they asked that its operator ship the device to her home.

On Oct. 27, 2023, the FBI raided Chapman's laptop farm and found more than 90 computers.

Her secret hustle was over. In December, she was nearly out of money. She was facing serious federal charges, but she glossed things over for her "lovelies," the name she gave her followers on TikTok.

"I lost my job at the end of October and didn't get paid for that last month," she said. "Even though I have been applying to at least three to four jobs every day, I haven't found anything yet."

As the months dragged on, she tried selling coloring books on Amazon. She opened an Etsy shop. She started a GoFundMe to drum up rent money.

In August 2024, she moved into a homeless shelter in Phoenix. "I will be back soon," she said in her last TikTok, posted in October. "It's been a hell of a roller coaster." She continues to live at a shelter, her lawyer said.

This February she pleaded guilty to wire fraud, identity theft and money laundering charges. Her total earnings amounted to just under $177,000. Under the terms of her plea agreement, she faces a maximum of just over nine years in prison. She is set to be sentenced on July 16.

Write to Robert McMillan at robert.mcmillan@wsj.com and Dustin Volz at dustin.volz@wsj.com