

Forum:[Hack Forums](#)

Thread: [Americans sentenced for running 'laptop farms' for North Korea](#)

MadScientist - May 9, 2026, 5:44 pm

Two U.S. nationals were sentenced to 18 months in prison each for operating so-called laptop farms that helped North Korean IT workers fraudulently obtain remote employment at nearly 70 American companies.

Matthew Isaac Knoot and Erick Ntekereze Prince are the seventh and eighth U.S.-based "laptop farmers" sent to prison since the start of the year as part of a federal initiative targeting North Korea's illicit revenue generation schemes.

"These sentences hold accountable U.S. nationals who enabled North Korea's illicit efforts to infiltrate U.S. networks and profit on the back of U.S. companies," said Assistant Attorney General John A. Eisenberg on Wednesday. "These defendants helped North Korean IT workers' masquerade as legitimate employees, compromising U.S. corporate networks and helping generate revenue for a heavily sanctioned and rogue regime.

Knoot (who was arrested and charged in August 2024) ran a laptop farm from his Nashville residences between July 2022 and August 2023.

During the scheme, he received company-issued laptops addressed to a stolen identity ("Andrew M."), then installed unauthorized remote desktop software that allowed North Korean IT workers to appear as a legitimate U.S.-based employee.

Victim companies paid more than \$250,000 to IT workers associated with Knoot's operation, with the payments falsely reported to the Social Security Administration and the Internal Revenue Service under stolen identities.

Prince (who pleaded guilty to wire-fraud conspiracy in November) enabled at least three North Korean IT workers to obtain remote employment at U.S. companies from approximately June 2020 through August 2024, operating through his company, Taggcar Inc. Victim companies paid the IT workers hired with the help of Prince more than \$943,000 in salary, the majority of which was routed overseas.

Knoot also caused more than \$500,000 in auditing and remediation costs at victim companies, while Prince's actions caused more than \$1 million in remediation costs. In addition to their 18-month prison sentences, Knoot was ordered to pay \$15,100 in restitution and forfeit an additional \$15,100, and Prince was ordered to forfeit \$89,000.

The FBI has been warning about North Korean IT workers infiltrating U.S. firms since at least 2023 and repeatedly noted that North Korea maintains a large army of thousands of IT workers using identity theft to secure employment at hundreds of American companies each year.

In April, U.S. nationals Kejia Wang and Zhenxing Wang were also sent to prison for helping North Korean remote information technology (IT) workers to pose as U.S. residents.

Last July, a 50-year-old Christina Marie Chapman from Arizona was sentenced to 102 months in prison for running a laptop farm in her own home, as part of a scheme that helped North Korean IT

workers get hired by 309 U.S. companies while using stolen identities.

Read More -

<https://www.bleepingcomputer.com/news/security/americans-sentenced-for-running-laptop-farms-for-north-korea/>

DAL-SHA - May 10, 2026, 7:53 am

Interesting ! Never Heard of Laptop farms before this thread !

Deany - May 10, 2026, 8:37 am

Laptop farms and phone farms are popular in China lol. Shoulda tried it there I guess?

Mercury - May 10, 2026, 3:19 pm

Hopefully they get tried for treason and receive maximum sentences. Nothing good ever comes out of anything that is related to North Korea. How the world has tolerated it for so long, is beyond me.

OG-Pablo - May 11, 2026, 2:34 am

(May 9, 2026 05:44 PM)MadScientist Wrote: [\[CITE\]](#) Two U.S. nationals were sentenced to 18 months in prison each for operating so-called laptop farms that helped North Korean IT workers fraudulently obtain remote employment at nearly 70 American companies.

Matthew Isaac Knoot and Erick Ntekereze Prince are the seventh and eighth U.S.-based "laptop farmers" sent to prison since the start of the year as part of a federal initiative targeting North Korea's illicit revenue generation schemes.

"These sentences hold accountable U.S nationals who enabled North Korea's illicit efforts to infiltrate U.S. networks and profit on the back of U.S. companies," said Assistant Attorney General John A. Eisenberg on Wednesday. "These defendants helped North Korean IT workers' masquerade as legitimate employees, compromising U.S. corporate networks and helping generate revenue for a heavily sanctioned and rogue regime.

Knoot (who was arrested and charged in August 2024) ran a laptop farm from his Nashville residences between July 2022 and August 2023.

During the scheme, he received company-issued laptops addressed to a stolen identity ("Andrew M."), then installed unauthorized remote desktop software that allowed North Korean IT workers to appear as a legitimate U.S.-based employee.

Victim companies paid more than \$250,000 to IT workers associated with Knoot's operation, with the payments falsely reported to the Social Security Administration and the Internal Revenue Service under stolen identities.

Prince (who pleaded guilty to wire-fraud conspiracy in November) enabled at least three North Korean IT workers to obtain remote employment at U.S. companies from approximately June 2020 through August 2024, operating through his company, Taggcar Inc. Victim companies paid the IT workers hired with the help of Prince more than \$943,000 in salary, the majority of which was routed overseas.

Knoot also caused more than \$500,000 in auditing and remediation costs at victim companies, while Prince's actions caused more than \$1 million in remediation costs. In addition to their 18-month prison sentences, Knoot was ordered to pay \$15,100 in restitution and forfeit an additional \$15,100, and Prince was ordered to forfeit \$89,000.

The FBI has been warning about North Korean IT workers infiltrating U.S. firms since at least 2023 and repeatedly noted that North Korea maintains a large army of thousands of IT workers using identity theft to secure employment at hundreds of American companies each year.

In April, U.S. nationals Kejia Wang and Zhenxing Wang were also sent to prison for helping North Korean remote information technology (IT) workers to pose as U.S. residents.

Last July, a 50-year-old Christina Marie Chapman from Arizona was sentenced to 102 months in prison for running a laptop farm in her own home, as part of a scheme that helped North Korean IT workers get hired by 309 U.S. companies while using stolen identities.

Read More -

<https://www.bleepingcomputer.com/news/security/americans-sentenced-for-running-laptop-farms-for-north-korea/>

This case highlights a serious cybersecurity and national security threat posed by North Korea's use of stolen U.S. identities to infiltrate American corporate networks. The operation of "laptop farms" by U.S. nationals like Knoot and Prince enables North Korean IT workers to bypass sanctions and generate illicit revenue while compromising sensitive company data. The use of stolen identities to mask the true origin of remote workers is a sophisticated form of fraud that undermines trust in remote employment. Financial damages extend beyond direct salary payments, including significant remediation and auditing costs imposed on victim companies. This will go on for ever as long as AI is here to stay.

KtDan - June 16, 2026, 10:59 am

damn, this is wild bro