

DOJ moves to claim \$7.74 million tied to North Korean IT worker scheme

By Jonathan Greig

Published: 2025-06-06 · Archived: 2026-04-05 21:13:02 UTC

The Department of Justice has filed a civil forfeiture complaint in federal court in connection with more than \$7.74 million that was previously frozen and seized from North Koreans who allegedly obtained the money through the regime's illicit IT worker scheme.

The funds are connected to Sim Hyon Sop, a North Korean Foreign Trade Bank representative who was allegedly conspiring with the IT workers from the country to launder money obtained through their [illegal employment at U.S. companies](#). Sim was [indicted](#) in April 2023 after the federal government caught him attempting to launder the money.

“For years, North Korea has exploited global remote IT contracting and cryptocurrency ecosystems to evade U.S. sanctions and bankroll its weapons programs,” said Sue Bai, head of the Justice Department's National Security Division.

The attempt to confiscate the funds, filed Thursday, “reflects the Department's strategic focus on disrupting these illicit revenue schemes,” Bai said.

Court documents said the participants are able to send cryptocurrency back to North Korea by setting up accounts with fake identities, moving funds in a series of small transactions, converting funds to other forms of cryptocurrency, purchasing NFTs, and using U.S.-based accounts to legitimize the activity.

Once the funds are commingled with other cryptocurrency and successfully laundered, they are sent to North Korea through Sim or Kim Sang Man, another North Korean official who runs an IT company working out of North Korea's Ministry of Defense, the DOJ said.

The IT company, known as Chinyong, employs many North Korean IT workers who work in Russia and Laos. Many of the workers have been hired as developers, coders or as IT support staff at blockchain development companies and are paid in stablecoins such as USDC and USDT, the DOJ said.

Cryptocurrency firm TRM Labs [tracked](#) wallets associated with Sim and found more than \$24 million received between 2021 and 2023. His accounts on unnamed cryptocurrency platforms were opened using “forged Russian identity documents and accessed from Korean-language devices operating from the UAE and Russia.”

TRM Labs found that Sim and Kim “functioned as central clearinghouses for the illicit proceeds” — with Sim operating out of Dubai and Kim operating out of Vladivostok, Russia.

Sim held a wallet that received laundered funds from dozens of sources while Kim ran two accounts that collected and redistributed funds to Sim and other wallets.

A substantial portion of Sim’s wallet balance “was later transferred to an over-the-counter trader based in the UAE, who was sanctioned by OFAC in December 2024 for converting illicit crypto proceeds into fiat currency,” according to TRM Labs.

The Justice Department explained that the complaint and the indictments [charging](#) Sim are part of the larger “[DPRK RevGen: Domestic Enabler Initiative](#)” launched last year to disrupt the financial network built to support the North Korean IT worker scheme.

The scheme has brought in millions for the North Korean regime and [several Americans have been charged](#) for either [knowingly or unknowingly](#) helping them pretend to work from the U.S.

Roman Rozhavsky, assistant director of the FBI’s Counterintelligence Division, said its investigations have uncovered massive campaigns by North Korea to “defraud U.S. businesses by obtaining employment using the stolen identities of American citizens.”

Employment scammers continue to evolve in the tools they use. This week ChatGPT maker OpenAI [said it identified and banned](#) accounts “associated with what appeared to be multiple suspected deceptive employment campaigns.” The company said it couldn’t directly tie its discovery to North Korea, but the behavior appeared to be consistent with schemes backed by the regime.

 Recorded Future®

Know what matters.

Act first.

Get started



No previous article

No new articles



[Jonathan Greig](#)

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.

Source: <https://therecord.media/north-korea-it-worker-scams-doj-civil-forfeiture-claim>