PRESS RELEASE

Tennessee Man Pleads in Hacking U.S. Supreme Court, AmeriCorps, and VA Health System

Friday, January 16, 2026

For Immediate Release

U.S. Attorney's Office, District of Columbia
USADC.Media@usdoj.gov

WASHINGTON – Nicholas Moore, 24, of Springfield, Tennessee, pleaded guilty this morning in U.S. District Court in connection with hacking the electronic filing system of the U.S. Supreme Court at least 25 times and additionally hacking accounts at AmeriCorps and the Veterans Administration Health System, announced U.S. Attorney Jeanine Ferris Pirro.

Moore pleaded guilty to a one count information charging him with fraud activity in connection with computers, a Class A misdemeanor. Moore is eligible for up to one year in prison and a fine of up to $100,000 when he is sentenced by Judge Beryl A. Howell on April 17.

According to court documents, the electronic filing system was restricted to authorized users. Between Aug. 29, 2023, and Oct. 22, 2023, Moore accessed the filing system without authorization using the stolen credential of an authorized user over 25 days, sometimes returning to the site multiple times on the same day.

On three occasions, Moore posted screenshots to his Instagram account, @ihackedthegovernment, of his victim's Supreme Court filing system details including the victim's name and other information.

Moore also used the stolen credentials of an authorized user of MyAmeriCorps to access a second victim's AmeriCorps account. Between Aug. 17, 2023, and Oct. 13, 2023, Moore obtained the second victim's personal information from the AmeriCorps servers. On Oct. 17, 2023, Moore posted that victim's personal information to the @ihackedthegovernment Instagram account.

Additionally, Moore used the stolen login credentials of a U.S. Marine Corps veteran to access the Department of Veterans Affairs "MyHealthEVet" platform on five days between Sept. 14, 2023, and Oct. 14, 2023. The hack allowed Moore to access the veteran's private health information including prescribed medications and other intimate data. Moore then posted the veterans' health information to @ihackedthegovernment and boasted about gaining access to the VA's servers.

This case was investigated by the Supreme Court of the United States Police - Protective Intelligence Unit and the FBI Washington Field Office with assistance from the U.S. Department of Veterans Affairs Office of Inspector General, and the AmeriCorps Office of Inspector General.

The matter is being prosecuted by Assistant U.S. Attorneys John Borchert and Rami Sibay for the District of Columbia.

26cr3

Contact
USADC.Media@usdoj.gov

Updated January 16, 2026

Topic

CYBERCRIME

Components

Federal Bureau of Investigation (FBI) | Office of the Inspector General | USAO - District of Columbia

Press Release Number: 26-26cr3

Related Content

PRESS RELEASE

Guilty Plea and Superseding Indictment

PRESS RELEASE

Cryptocurrency Money Launderer Pleads Guilty to

PRESS RELEASE

Ukrainian Pleads Guilty in DC in Laptop Farm Scheme

Announced in Social Engineering Scheme that Stole $263 Million in Cryptocurrency

Evan Tangeman, 22, of Newport Beach, California, pleaded guilty today in connection with his role in a multi-state conspiracy that used social engineering to steal hundreds of millions of dollars...

December 8, 2025

RICO Conspiracy in Scheme that Stole $263 Million in Crypto

Kunal Mehta, 45, of Irvine, California, pleaded guilty today in connection with his role in a multi-state conspiracy that used social engineering to steal hundreds of millions of dollars in...

November 18, 2025

That Generated Income for North Korean IT Workers

Oleksandr Didenko, 28, of Kyiv, Ukraine, pleaded guilty November 10 in U.S. District Court in connection with a years-long scheme that stole the identities of U.S. citizens and sold them...

November 13, 2025

District of Columbia

Main Office:
601 D Street, NW
Washington, DC

Email USAO-DC

Telephone: (202) 252-7566