UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA v. NICHOLAS MOORE, Defendant.	CRIMINAL NO.

STATEMENT OF THE OFFENSE

Pursuant to Federal Rule of Criminal Procedure 11, the United States, by and through its undersigned attorney, and the defendant, **NICHOLAS MOORE ("MOORE")**, with the concurrence of his attorney, Eugene Ohm, Esq., stipulate and agree that the following facts fairly and accurately describe **MOORE's** conduct in the offense to which he is pleading guilty. These facts do not constitute all of the facts known to the parties concerning the charged offenses and related conduct. This statement is being submitted to demonstrate that sufficient facts exist to establish that **MOORE** committed the offense to which he is pleading guilty. **MOORE** knowingly, voluntarily, and truthfully admits to the facts set forth below.

I. Maximum Penalties

As to Count One, a violation of 18 U.S.C. § 1030(a)(2) carries a maximum sentence of one year of imprisonment; a fine not to exceed $100,000, pursuant to 18 U.S.C. § 3571(b); a term of supervised release of not more than one year, pursuant to 18 U.S.C. § 3583(b)(3); and an obligation to pay any applicable interest or penalties on fines and restitution not timely made.

II. Elements of the Offense

As to Count One, the elements of the charged offense, a violation of 18 U.S.C. § 1030(a)(2), are:

1) The defendant intentionally accessed a computer;

2) The access was without authorization;

3) The defendant thereby obtained information; and

4) The information was from a protected computer, including a computer which was used in or affected interstate commerce or communication.

III. Brief Statement of Facts

The United States Supreme Court's Servers

1. The Supreme Court of the United States used an internet-based electronic filing system to receive and store electronic versions of documents filed with the Court. In certain circumstances, filings made on the electronic filing system were posted to the Court's public docket without review or action by the Court's Clerk's Office. The electronic filing system operated on computer servers located in Washington, D.C. These servers were used in and affected interstate commerce and communication.

2. Access to the electronic filing system was restricted to authorized users. **MOORE** was not an authorized user. Nevertheless, between August 29 and October 22, 2023, **MOORE** intentionally accessed the Supreme Court's electronic filing system without authorization using the stolen credentials of an authorized user ("GS") on 25 different days, sometimes returning to the site multiple times on the same day.

3. **MOORE** thereby obtained personal information about GS that was saved on the Supreme Court's electronic filing system servers, including GS's full name, email address, phone number, home address, date of birth, and the private answers GS had given to three security questions.

4. On July 29, August 18, and November 28, 2023, **MOORE** publicly posted on his Instagram account, which used the handle "@ihackedthegovernment," screenshots of GS's home page on the Supreme Court electronic filing system. Clearly visible to the public in the screenshots

were GS's name and a list of all of GS's current and past electronic filing records.

AmeriCorps' Servers

5. Operating under the name AmeriCorps, the Corporation for National and Community Service is a federal agency that promotes national service, connecting tens of thousands of Americans each year to non-profits, public agencies, and community organizations to meet community needs in education, the environment, public safety, health, and homeland security. AmeriCorps operated an internet-based platform known as the "My AmeriCorps" portal that allowed current, former, and prospective AmeriCorps members to apply for programs and track their benefits. MyAmeriCorps operated on computer servers located in Washington, D.C. and Virginia. These servers were used in and affected interstate commerce and communication.

6. Between August 17 and October 13, 2023, **MOORE** used the stolen credentials of an authorized MyAmeriCorps user ("SM") to access SM's AmeriCorps account seven times. In doing so, **MOORE** obtained from AmeriCorps' servers SM's personal information, including his date of birth, social security number, email address, home address, phone number, citizenship status, veteran status, and service history.

7. On October 17, 2023, **MOORE** publicly posted on his "@ihackedthegovernment" Instagram account screenshots boasting about his access to AmeriCorps' servers and to SM's personal information. This post displayed to the public SM's name, date of birth, email address, home address, phone number, citizenship status, veteran status, service history, and the last four digits of his social security number.

The Department of Veterans' Affairs Servers

8. The Department of Veteran's Affairs ("VA") is a department of the United States whose mission is to care for those who have served in our nation's military and for their families, caregivers, and survivors. The VA operated an internet-based platform known as "My

HealtheVet." This platform allowed veterans to manage their health care, including refilling prescriptions, viewing medical records, communicating with their health care team through secure messaging, and managing appointments. The MyHealtheVet platform operated on computer servers located in various jurisdictions in the United States. These servers are used in and affected interstate commerce and communication.

9. Between September 14, 2023 and October 14, 2023, **MOORE** used the stolen login credential of an authorized user ("HW") – a veteran who served in the United States Marine Corps – to access the Department of Veteran's Affairs "MyHealtheVet" platform on five different days. In doing so, **MOORE** obtained private information about HW from the VHA, including highly sensitive health information about the medications HW had been prescribed. **MOORE** also obtained HW's blood type, email address, physical address, and phone number.

10. On October 13, 2023, **MOORE** disclosed HW's individually identifiable health information when he sent an associate a screenshot from HW's MyHealtheVet account that identified HW and showed the medications he had been prescribed.

11. On October 15 and October 16, 2023, **MOORE** publicly posted on his Instagram account @ihackedthegovernment screenshots boasting of his access to the VA's servers and to HW's personal information. These posts displayed to the public HW's personal information, including his full name, home address, service branch, email address, phone number, and blood type.

Respectfully submitted,

JEANINE PIRRO
United States Attorney

By: */s/ Rami Sibay*
Rami Sibay
Special Assistant United States Attorney

DEFENDANT'S ACCEPTANCE

I have read the foregoing Statement of Offense, and I have discussed it fully with my attorney, Eugene Ohm. I fully understand this proffer and I acknowledge its truthfulness, agree to it, and accept it without reservation. I do this voluntarily and of my own free will, intending to be legally bound. No threats have been made to me nor am I under the influence of anything that could impede my ability to understand this proffer fully.

Date: 1/8/26

× _____
Nicholas Moore
Defendant

ATTORNEY'S ACKNOWLEDGMENT

I have read every page constituting the government's statement of offense related to my client's guilty plea. I have reviewed the entire proffer with my client, Nicholas Moore, and have discussed it with him fully. I concur in my client's agreement with and acceptance of this proffer.

Date: 1/8/26

_____
Eugene Ohm
Attorney for Defendant