

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

MICHAEL CHARLES SCHENA,

Defendant.

Case No. 1:25-mj-143

AFFIDAVIT IN SUPPORT OF APPLICATION FOR CRIMINAL COMPLAINT

I, Adam Meredith, being duly sworn, hereby depose and state:

BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), and have been so employed since December 2022. I presently am assigned to the Washington Field Office and am tasked with investigating a variety of offenses involving espionage, and the unlawful retention or disclosure of classified information. During my time at the FBI Academy, Quantico, Virginia, I have received training in a variety of investigative and legal matters, including the drafting of search warrant affidavits, and probable cause. I have also received training specific to counterintelligence and espionage investigations. Based on my experience I am familiar with efforts used to unlawfully collect and disseminate sensitive government information, including national defense information, and with the tradecraft used by intelligence services and their officers. As a Federal Agent, I am authorized to investigate violations of laws of the United States and, as a law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

2. This affidavit is submitted in support of an application for a criminal complaint charging Michael Charles Schena (hereinafter, "SCHENA") with conspiracy to gather, transmit, or lose defense information, in violation of Title 18, United States Code, Sections 793(e) and (g).

3. The facts set forth in this affidavit are based on my personal knowledge and review of records, documents, and other physical evidence obtained during this investigation, as well as information conveyed to me by other law enforcement officials. This affidavit does not include each and every fact observed by me or known to the government. I have set forth only those facts necessary to support a finding of probable cause.

STATUTORY AUTHORITY AND DEFINITIONS

4. Under 18 U.S.C. § 793(e), "[w]hoever having unauthorized possession of, access to, or control over any document . . . or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted" or attempts to do or causes the same "to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it" shall be fined or imprisoned not more than ten years, or both.

5. Section 793(g) provides, "If two or more persons conspire to violate any of the foregoing provisions of this section, and one or more of such persons do any act to effect the object of the conspiracy, each of the parties to such conspiracy shall be subject to the punishment provided for the offense which is the object of such conspiracy.

6. National security information is information owned by, produced by, produced for, and under the control of the United States government. Pursuant to Executive Order 12958

signed on April 17, 1995, as amended by Executive Order 13292 on March 25, 2003, and Executive Order 13526 on December 29, 2009, national security information is classified as “TOP SECRET,” “SECRET,” or “CONFIDENTIAL,” as follows:

- a. Information is classified as TOP SECRET if the unauthorized disclosure of that information reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority was able to identify or describe.
- b. Information is classified as SECRET if the unauthorized disclosure of that information reasonably could be expected to cause serious damage to the national security that the original classification authority was able to identify or describe.
- c. Information is classified as CONFIDENTIAL if the unauthorized disclosure of that information reasonably could be expected to cause damage to the national security that the original classification authority was able to identify or describe.

7. Classified information is marked according to its classification, following standard formats for different types of media, including headers and footers stating the highest classification level.

8. Pursuant to Executive Order 13526, information classified at any level can be lawfully accessed only by persons determined by an appropriate United States government official to be eligible for access to classified information, who have signed an approved non-disclosure agreement, who receive a security clearance, and who have a “need to know” the classified information. Classified information can only be stored or discussed in an approved facility and approved systems.

SCHENA’S BACKGROUND

9. SCHENA is employed by the United States Department of State (“DOS”) as a South Caribbean Desk Officer in the Bureau of Western Hemisphere America, located at DOS Headquarters in Washington, DC. During the relevant periods discussed below, SCHENA held a TOP SECRET security clearance.

10. On January 9, 2006, SCHENA signed a Classified Information Nondisclosure Agreement acknowledging, among other things, that he has received a security indoctrination concerning the nature and protection of classified information. Further, in that agreement SCHENA agreed that he had been advised that any breach may, among other penalties, constitute violation(s) of United States criminal laws, not limited to Sections 641, 793, 794, 798, 952 and 1924, Title 18, United States Code. SCHENA has access to materials classified up to the SECRET level while in his physical workspace at DOS located in Washington, D.C. However, SCHENA also conducts work from his home in Alexandria, Virginia where he can access information classified up to the Sensitive But Unclassified (SBU) level from his DOS issued laptop computer.

PROBABLE CAUSE

11. Beginning in or about April 2022, SCHENA has been communicating with people he met online through various communication platforms and provided information to which they were not entitled. In return, SCHENA has received payments for the provision of this information.

12. For example, on or about April 11, 2022, SCHENA received a message on a social media platform from a user on the platform (Platform User 1) who stated they worked for an international consulting company and inquired about SCHENA's interest in working with them. SCHENA replied indicating his interest. Over the next couple of weeks, SCHENA and Platform User 1 attempted to schedule video teleconference calls and identify a successful method for Platform User 1 to pay SCHENA. On May 18, 2022, Platform User 1 attempted to pay SCHENA \$100 five (5) times but the transactions failed. Shortly thereafter, another attempted payment was made for \$500 which was successfully deposited. Approximately six hours after that payment was made, Platform User 1 asked SCHENA to resend the "pictures" with a higher quality resolution.

Based on my training and experience, this payment of \$500 is for the submission of information or photographs of information to Platform User 1.

13. On or about June 19, 2022, SCHENA emailed Platform User 1 the text from a State Department document, which had (SBU) markings. However, SCHENA removed some, but not all, (SBU) markings from the document prior to sending it to Platform User 1. Approximately two days later, on June 21, 2022, SCHENA received an online payment of \$500. SCHENA was not authorized to disclose sensitive U.S. government information to Platform User 1.

14. Between in or about May 2022 and in or about March 2023, SCHENA received payments from various account names, at least ten transactions of which, based on FBI investigation, relate to the people SCHENA was engaging with online, including those noted above. The notes for five of the received payments included a reference of "from Jason."

15. Next, according to information obtained from SCHENA's iCloud, SCHENA had an invoice for the receipt of "10,000 USD and an iPhone 14 mobile device from Jason, which equals 79841 CNY." The invoice is dated August 30, 2024. CNY is believed to be a reference to the Chinese yuan renminbi, the official currency of the People's Republic of China. Based on my training and experience, I believe the referenced iPhone 14 was intended as a covert communication device for SCHENA to image and/or transmit information without law enforcement detection to others who are not otherwise authorized to receive it.

16. On or about February 17, 2025, SCHENA accessed the DOS system from Alexandria, Virginia, within the Eastern District of Virginia, and downloaded a document visibly marked as SBU. SCHENA then attempted to email the document from his DOS email account to his personal email account. However, after receiving an alert that emailing the sensitive but unclassified information may violate DOS policy, SCHENA classified his email as Unclassified.

He then sent the email to his personal email account. SCHENA then deleted the downloaded SBU document from his work issued computer and logged off.


17. Based on camera surveillance, on February 27, 2025, SCHENA logged into the DOS classified enclave CLASSNET at his computer workstation in his DOS workspace. SCHENA accessed at least five documents relating to the diplomatic relationship of the U.S. The documents were all visibly marked with the SECRET classification markings. SCHENA then photographed the documents, which were displayed on his computer screen, with a white mobile telephone.

18. SCHENA then opened an application on his white mobile telephone and typed what appeared to be a message in an application. SCHENA then appeared to insert the photographs that he had just taken into the messages. SCHENA then deleted the photographs from the camera roll of his white mobile telephone. Shortly thereafter, SCHENA left DOS and proceeded towards his home. SCHENA was stopped outside of his residence in Alexandria, Virginia and was still in possession of the white mobile telephone, which is an Apple iPhone 14 registered with a foreign telephone number. The agency that classified five of the documents SCHENA took photographs of has confirmed that the documents are currently classified.

CONCLUSION

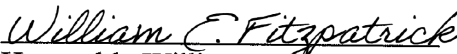
19. Based on the foregoing and my training and experience, I submit there is probable cause to believe that between April 2022 continuing through February 28, 2025, Michael SCHENA, and others, knowingly and unlawfully conspired together and with each other to obtain and transmit documents, writings, photographs, instruments, application, and notes relating to the national defense of the United States (“national defense information”) to an individual or individuals not entitled to receive it in violation of 18 U.S.C. §§ 793 (e) and (g).

20. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.



Adam Meredith
Special Agent
Federal Bureau of Investigation

Sworn and subscribed to me this 3rd day of March 2025.


Honorable William E. Fitzpatrick
United States Magistrate Judge