NICOLA T. HANNA
United States Attorney
BRANDON D. FOX
Assistant United States Attorney
Chief, Criminal Division
JULIAN L. ANDRÉ (Cal. Bar No. 251120)
Assistant United States Attorney
Major Frauds Section
1100 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-6683
Facsimile: (213) 894-6269
E-mail: Julian.L.Andre@usdoj.gov

DANIEL A. KAHN
Acting Chief, Fraud Section
Criminal Division, U.S. Department of Justice
CHRISTOPHER FENTON
Trial Attorney, Fraud Section
Criminal Division, U.S. Department of Justice
1400 New York Avenue NW, 3rd Floor
Washington, DC 20530
Telephone: (202) 302-0539
Facsimile: (202) 514-0152
E-mail: Christopher.Fenton@usdoj.gov

Attorneys for Plaintiff
UNITED STATES OF AMERICA

UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, v. RICHARD AYVAZYAN, aka “Richard Avazian” and “Iuliia Zhadko,” MARIETTA TERABELIAN, aka “Marietta Abelian” and “Viktoria Kauichko,” ARTUR AYVAZYAN, aka “Arthur Ayvazyan,” and TAMARA DADYAN, Defendants.	No. CR 20-579-SVW *EX PARTE* APPLICATION FOR A PROTECTIVE ORDER REGARDING DISCOVERY CONTAINING PERSONAL IDENTIFYING INFORMATION, ACCESS DEVICE MATERIALS, AND PRIVACY ACT INFORMATION *[PROPOSED] ORDER FILED CONCURRENTLY HEREWITH*

Pursuant to Federal Rule of Criminal Procedure 16(d)(1), plaintiff United States of America, by and through its counsel of record, the United States Attorney for the Central District of California, Assistant United States Attorney Julian L. André, and Department of Justice Trial Attorney Christopher Fenton, hereby applies ex parte for a protective order regarding discovery containing personal identifying information, unauthorized and counterfeit access devices, and privacy act information.

The proposed protective order is necessary so that the government can begin producing discovery to defense counsel in this matter. The discovery in this COVID-19-related fraud and identity theft case contains an extensive volume of personal identifying information ("PII") of third-parties, witnesses, and victims. The discovery also includes significant volumes of unauthorized or counterfeit access devices, including social security numbers, employee identification numbers, drivers' license numbers, and bank and credit card numbers, some of which was used to perpetrate the alleged fraud or which could be used to engage in additional fraudulent conduct. Producing this sensitive information without limitation risks the privacy and security of victims, other third-parties, and the public in general. Moreover, allowing the defendants in this case, two of whom have prior felony fraud convictions in this district, to possess such PII and access devices would pose a significant risk of harm to victims, other third-parties, and the public in general. The proposed stipulation will ensure that defendants' counsel can access the discovery and review it with the defendants, while preventing the defendants from

possessing and improperly using this sensitive and confidential information for improper or illegal purposes.

This application is based upon attached the declaration of Assistant United States Attorney Julian L. André, the concurrently filed proposed protective order, the files and records in this case, and such further evidence and argument as the Court may permit.

On November 30, 2020, the government provided counsel for each defendant with a proposed stipulation regarding a protective order in this case. The government conferred with counsel for defendant RICHARD AYVAYZAN ("R. AYVAZYAN") regarding the terms of a protective order, but was unable to reach an agreement. Although defendant MARIETTA TERABELIAN stipulated to the entry of an appropriate protective order (CR 50), defendant TERABELIAN subsequently withdrew her stipulation.[1] Counsel for defendants TAMARA DADYAN and ARTUR AYVAZYAN have yet to respond to the government's proposed stipulation for a protective order.

On December 7, 2020, the government notified counsel for each defendant via email that it intended to file the instant ex parte application and requested they advise the government whether they oppose the ex parte nature of this application. Counsel for defendant TERABELIAN, A. AYVAZYAN, and DADYAN have not yet responded to the government's email. At approximately 5:02 p.m. on December 7, 2020, counsel for defendant R. AYVAZYAN responded via email that

[1] Despite certifying that he had reviewed the stipulation and proposed protective order with his client and agreed to its terms (CR 50-1), counsel for defendant TERABELIAN has now indicated that he mistakenly thought that the government's proposed protective order was the same as a protective order counsel for defendant RICHARD AYVAZYAN had previously drafted and circulated to the other defendants' counsel without the government's knowledge or consent.

defendant R. AYVAZYAN would be filing at 5:05 p.m. its own ex parte application to compel production of discovery in this matter.

Dated: December 7, 2020

Respectfully submitted,

NICOLA T. HANNA
United States Attorney

BRANDON D. FOX
Assistant United States Attorney
Chief, Criminal Division

/s/
JULIAN L. ANDRÉ
Assistant United States Attorney
CHRISTOPHER FENTON
Department of Justice Trial Attorney

Attorneys for Plaintiff
UNITED STATES OF AMERICA

DECLARATION OF JULIAN L. ANDRÉ

I, Julian L. André, declare as follows:

1. I am an Assistant United States Attorney for the Central District of California. Together with Department of Justice Trial Attorney Christopher Fenton, I represent the government in United States v. Richard Ayvazyan et al., CR No. 20-579-SVW. I make this declaration in support of the government's ex parte application to obtain a protective order regarding discovery containing personal identifying information ("PII"), unauthorized and counterfeit access devices, and privacy act information.

The Need for a Protective Order

2. A protective order is necessary because the government intends to produce to the defense materials containing third parties' PII, including PII relating to victims and other third parties. The government also intends to produce materials that constitute or depict unauthorized or counterfeit access devices, including access devices which were used to perpetrate the alleged fraud or could be used to engage in additional fraudulent conduct. The government believes that disclosing this sensitive information without limitation risks the privacy and security of the information's legitimate owners, and may expose victims, other third parties and the general public to potential safety risks. Indeed, courts have already considered the risks these defendants pose in this respect and determined to prohibit the defendants from possessing such information as a condition of release. Moreover, the government has an ongoing obligation to protect these victims and other third-parties, as well as the general public. The government therefore cannot simply produce to defendants an unredacted set of discovery

containing this sensitive information, particularly in light of the alleged criminal conduct in this case and defendant R. AYVAZYAN's and defendant TERABELIAN's prior federal fraud convictions involving allegations similar to those alleged here.

3. Moreover, PII and unauthorized or counterfeit access devices make up a significant part of the discovery in this case and such information itself, in many instances, has evidentiary value. If the government were to attempt to redact all this information in strict compliance with Federal Rule of Criminal Procedure 49.1, the Central District of California's Local Rules regarding redaction, and the Privacy Policy of the United States Judicial Conference, the defense would receive a set of discovery that would be highly confusing and difficult to understand, and it would be challenging for defense counsel to adequately evaluate the case, provide advice to defendant, or prepare for trial. Redacting such information would also be unduly time-consuming and could lead to delays in the production of discovery.

4. An order is also necessary because the government intends to produce to the defense materials that may contain information within the scope of the Privacy Act, 5 U.S.C. § 552a ("Privacy Act Information"). To the extent that these materials contain Privacy Act Information, an order is necessary to authorize disclosure pursuant to 5 U.S.C. § 552a(b)(11).

5. The purpose of the Protective Order is to (a) allow the government to comply with its discovery obligations while preventing the unauthorized dissemination, distribution, use of this sensitive information; and (b) provide the defense with sufficient information to adequately represent defendant.

Background Information

6. On November 17, 2020, a federal grand jury returned a 12-count indictment in United States v. Ayvazyan et al., No. CR 20-579-SVW. The indictment charges defendant RICHARD AYVAZYAN ("R. AYVAZYAN"), defendant MARIETTA TERABELIAN, defendant ARTUR AYVAZYAN ("A. AYVAYZAN"), and defendant TAMARA DADYAN with violations of 18 U.S.C. § 1349 (conspiracy to commit wire and bank fraud); 18 U.S.C. § 1343 (wire fraud); and 18 U.S.C. § 1344(2) (bank fraud). (CR 32.) Defendant R. AYVAZYAN is also charged with a violation of 18 U.S.C. § 1028A(a)(1) (aggravated identity theft). (Id.)

7. All four defendants are currently released on bond pending trial. The conditions of defendants' release preclude them from using or possessing "any identification, mail matter, access devices, or any identification-related material other than in [their] own legal or true name[s]," and using bank accounts or credit card accounts except in their true names. (See CR 5.)

8. The charges in this case arise from a conspiracy to fraudulently obtain millions of dollars in COVID-19-related disaster relief funds under the Paycheck Protection Program ("PPP") and Economic Injury Disaster Loan Program ("EIDL"). (CR 32.) Among other things, the indictment alleges that the defendants used fake, stolen, and synthetic identities, as well as stolen or fictitious business names, to submit fraudulent PPP and EIDL loan applications to financial institutions and the Small Business Administration ("SBA"). (Id.) In connection with the fraudulent loan applications, defendants would also make false statements and submit fake documents, including fake Internal Revenue Service ("IRS") forms and fake California Drivers' Licenses ("CA DL"). (Id.) The indictment

further alleges that defendants used the fraudulently obtained disaster relief funds for their own personal benefit, including to purchase the $3.25 million luxury home in which defendants R. AYVAZYAN and TERABELIAN currently reside. (Id.)

9. In 2012, defendants R. AYVAZYAN and TERABELIAN were previously convicted in this district of conspiracy to commit bank fraud, in violation of 18 U.S.C. § 371. See United States v. Ayvazyan et al., No. SA CR 11-180-CJC, Dkt. Nos. 58, 90, 99.

Discovery to be Produced

10. As part of its investigation in this case, the government is in possession of documents relating to the charges against defendants, and seeks to provide those documents to counsel for defendants (although some of the materials may exceed the scope of the government's discovery obligations).

11. Many of the materials that the government intends to disclose as discovery in this case contains extensive PII and unauthorized and counterfeit access device information, including the following:

a. PII of real persons, including victims, other third-parties and witnesses, as well as PII relating to co-defendants and potential co-conspirators. Such information includes, among other things, names, dates of birth, addresses, phone numbers, email addresses, Social Security numbers, drivers' license numbers, credit card and bank account information, and personal online passwords.

b. Unauthorized and counterfeit access devices relating to stolen, fake, and synthetic identities, including Social Security numbers, drivers' license numbers, bank or credit card account numbers, and personal online passwords.

c. Financial records, including bank records, credit card records, and loan applications, containing PII relating to real persons, such as names, dates of birth, addresses, phone numbers, email addresses, tax information, Social Security numbers, drivers' license numbers, account numbers, and other confidential financial information.

d. Telephone and internet service provider ("ISP") records, containing PII relating to real persons, such as names, addresses, phone numbers, mobile identification numbers, and email addresses.

e. Credit reports relating to real persons.

f. Records and information obtained from government agencies, including the IRS and California Employment Development Department ("CA EDD").

12. The government also seized physical evidence and a number of digital devices during the execution of search warrants in connection with its investigation, which it intends to produce to defendants once the evidence has been processed by law enforcement. I understand that the physical and digital evidence seized contains a substantial amount of PII relating to third-parties, as well as unauthorized or counterfeit access devices which was either used in connection with the alleged fraud or which could be used for further fraudulent activity. For example, I understand that a cellphone belonging to defendant R. AYVAZYAN contained, among other things, numerous counterfeit and unauthorized access devices, namely, drivers' license numbers, Social Security numbers, and credit card numbers relating to real, fake, and synthetic identities. Similarly, I understand that at least 20 real or fake drivers' licenses and

Social Security cards were seized from the residence of defendants A. AYVAZYAN and DADYAN.

The Proposed Protective Order

13. The proposed protective order filed concurrently herewith, contains the following provisions designed to prevent the unauthorized distribution, dissemination, and use of PII and access devices materials:

a. As used herein, "PII Materials" includes any information that can be used to identify a person, including a name, address, date of birth, Social Security number, driver's license number, telephone number, account number, email address, personal identification number, and financial information.

b. As used herein, "Access Device Materials" includes any materials that constitute or depict unauthorized or counterfeit access devices, as defined in 18 U.S.C. § 1029(e).

c. "Confidential Information" refers to any document or information containing PII Materials or Access Device Materials that the government produces to the defense pursuant to this Protective Order and any copies thereof.

d. "Defense Team" includes (1) defendant's counsel of record ("defense counsel"); (2) other attorneys at defense counsel's law firm who may be consulted regarding case strategy in this case; (3) defense investigators who are assisting defense counsel with this case; (4) retained experts or potential experts; and (5) paralegals, legal assistants, and other support staff to defense counsel who are providing assistance on this case. The Defense Team does not include defendant, defendant's family members, or any other associates of defendant.

e. The government is authorized to provide defense counsel with Confidential Information marked with the following legend: "CONFIDENTIAL INFORMATION -- CONTENTS SUBJECT TO PROTECTIVE ORDER." The government may put that legend on the digital medium (such as DVD or hard drive) or simply label a digital folder on the digital medium to cover the content of that digital folder. The government may also redact any PII contained in the production of Confidential Information.

f. If defendant objects to a designation that material contains Confidential Information, the parties shall meet and confer. If the parties cannot reach an agreement regarding defendant's objection, defendant may apply to this Court to have the designation removed.

g. Defendant and the Defense Team shall use the Confidential Information solely to prepare for any pretrial motions, plea negotiations, trial, and sentencing hearing in this case, as well as any appellate and post-conviction proceedings.

h. The Defense Team shall not permit anyone other than the Defense Team to have possession of Confidential Information, including defendant, while outside the presence of the Defense Team.

i. At no time, under no circumstance, will any Confidential Information be left in the possession, custody, or control of defendant, regardless of defendant's custody status.

j. Defendant may review PII Materials or Access Device Materials only in the presence of a member of the Defense Team, who shall ensure that defendant is never left alone with any PII Materials or Access Device Materials. At the conclusion of any meeting with defendant at which defendant is permitted to view PII

Materials or Access Device Materials, defendant must return any PII Materials or Access Device Materials to the Defense Team, and the member of the Defense Team present shall take all such materials with him or her. Defendant may not take any PII Materials or Access Device Materials out of the room in which defendant is meeting with the Defense Team.

k. Defendant may see and review Confidential Information as permitted by this Protective Order, but defendant may not copy, keep, maintain, or otherwise possess any Confidential Information in this case at any time. Defendant also may not write down or memorialize any data or information contained in the Confidential Information.

l. The Defense Team may review Confidential Information with a witness or potential witness in this case, including defendant. A member of the Defense Team must be present if PII Materials or Access Device Materials are being shown to a witness or potential witness. Before being shown any portion of Confidential Information, however, any witness or potential witness must be informed of, and agree in writing to be bound by, the requirements of the Protective Order. No member of the Defense Team shall permit a witness or potential witness to retain Confidential Information or any notes generated from Confidential Information.

m. Due to the impact of the COVID-19 pandemic, the Defense Team may use secure video conferencing applications, such as Zoom, WebEx, Microsoft Teams, or Blue Jeans, to review Confidential Information with a defendant or witness, provided that Defense Team certifies in writing that there is no way for the defendant or witness to (i) maintain electronic copies of the Confidential

Information once the video conference is over; or (ii) photograph, record, write down or otherwise memorialize any data or information contained in the Confidential Information.

n. The Defense Team shall maintain Confidential Information safely and securely, and shall exercise reasonable care in ensuring the confidentiality of those materials by (1) not permitting anyone other than members of the Defense Team, defendant, witnesses, and potential witnesses, as restricted above, to see Confidential Information; (2) not divulging to anyone other than members of the Defense Team, defendant, witnesses, and potential witnesses, the contents of Confidential Information; and (3) not permitting Confidential Information to be outside the Defense Team's offices, homes, vehicles, or personal presence.

o. To the extent that defendant, the Defense Team, witnesses, or potential witnesses create notes that contain, in whole or in part, Confidential Information, or to the extent that copies are made for authorized use by members of the Defense Team, such notes, copies, or reproductions become Confidential Information subject to the Protective Order and must be handled in accordance with the terms of the Protective Order.

p. The Defense Team shall use Confidential Information only for the litigation of this matter and for no other purpose. Litigation of this matter includes any appeal filed by defendant and any motion filed by defendant pursuant to 28 U.S.C. § 2255. In the event that a party needs to file Confidential Information with the Court or divulge the contents of Confidential Information in court filings, the filing should be made under seal. If the Court rejects the request to file such information under seal, the party seeking to

file such information publicly shall provide advance written notice to the other party to afford such party an opportunity to object or otherwise respond to such intention. If the other party does not object to the proposed filing, the party seeking to file such information shall redact any PII Materials or Access Device Materials and make all reasonable attempts to limit the divulging of PII Materials or Access Device Materials.

q. Any Confidential Information inadvertently produced in the course of discovery prior to entry of the Protective Order shall be subject to the terms of this Protective Order. If Confidential Information was inadvertently produced prior to entry of the Protective Order without being marked "CONFIDENTIAL INFORMATION -- CONTENTS SUBJECT TO PROTECTIVE ORDER," the government shall reproduce the material with the correct designation and notify defense counsel of the error. The Defense Team shall take immediate steps to destroy the unmarked material, including any copies.

r. Confidential Information shall not be used by any member of the defense team, in any way, in any other matter, absent an order by this Court. All materials designated subject to the Protective Order maintained in the Defense Team's files shall remain subject to the Protective Order unless and until such order is modified by this Court. Upon request by the government, defense counsel shall return all PII Materials and Access Device Materials, certify that such materials have been destroyed, or certify that such materials are being kept pursuant to the California Business and Professions Code and the California Rules of Professional Conduct.

s. In the event that there is a substitution of counsel prior to when such documents must be returned, new defense counsel

must be informed of, and agree in writing to be bound by, the requirements of the Protective Order before defense counsel transfers any Confidential Information to the new defense counsel. New defense counsel's written agreement to be bound by the terms of the Protective Order must be returned to the Assistant U.S. Attorney assigned to the case. New defense counsel then will become the Defense Team's custodian of materials designated subject to the Protective Order and shall then become responsible, upon the conclusion of appellate and post-conviction proceedings, for returning to the government, certifying the destruction of, or retaining pursuant to the California Business and Professions Code and the California Rules of Professional Conduct all PII Materials or Access Device Materials.

t. Defense counsel shall advise defendant and all members of the Defense Team of their obligations under the Protective Order and ensure their agreement to follow the Protective Order, prior to providing defendant and members of the Defense Team with access to any materials subject to the Protective Order.

14. On November 30, 2020, prior to each defendant appearing for post-indictment arraignment, the government emailed each defendant's counsel a proposed stipulation for protective order that would cover the sensitive personal and financial information that comprises the vast majority of the discovery in this case. That proposed stipulation was based on the standard protective order the United States Attorney's Office adopted in March 2020 after consultations with the Office of the Federal Public Defender. The terms of the proposed protective order, including the terms precluding the defendants from possessing sensitive personal and financial

information, were also consistent with prior protective orders entered by this Court. See, e.g., Protective Order, United States v. Ohiri, No. CR 19-0042-SVW, Dkt. 35 (C.D. Cal. Mar. 14, 2019). Except for the two modifications described in paragraph 21 below, the terms of the protective order government sent defendants' counsel on November 30, 2020, were the same as the terms contained in the proposed protective order filed concurrently herewith and described in paragraph 13 above.

15. On November 30, 2020, counsel for defendant R. AYVAZYAN advised the government that it objected to the government's stipulation and proposed protective order. Most notably, counsel for defendant R. AYVAZYAN indicated that defendant R. AYVAZYAN objects to any provisions that would preclude him from possessing discovery in this matter, including the sensitive and confidential PII and access device materials described herein. In turn, the government advised defendant R. AYVAYZAN that due to the nature of the allegations against defendant R. AYVAZYAN, as well his prior federal fraud conviction, it would be inappropriate to allow defendant to possess personal identifying information ("PII") relating to third-parties or witnesses, or to possess unauthorized and counterfeit access devices. On December 2, 2020, the government and counsel for defendant R. AYVAZYAN met-and-conferred regarding the government's proposed protective order, but were unable to reach an agreement as to the terms of the protective order.

16. On November 30, 2020, counsel for defendant TERABELIAN signed the government's stipulation for protective order, stating "Defense Counsel has conferred with defendant regarding this stipulation and the proposed order thereon, and defendant agrees to

the terms of the proposed order." (CR 50 at 8.) On December 3, 2020, however, counsel for defendant TERABELIAN filed a notice indicating he was withdrawing the stipulation because he mistakenly thought that the protective order to which defendant TERABELIAN had agreed was the same as a protective order counsel for defendant R. AYVAZYAN had previously drafted and circulated to the other defendants in this case without the government's knowledge or consent. (CR 52.) The government understands that defendant TERABELIAN has now adopted the same objections previously raised by defendant R. AYVAZYAN.

17. The government understands that defendant A. AYVAZYAN is in the process of retaining counsel to represent him in this matter. The Office of the Federal Public Defender was appointed to represent defendant A. AYVAZYAN for the limited purpose of appearing at his initial appearance and post-indictment arraignment, and advised government counsel that any issues relating to the protective order would be addressed by retained counsel at a later date.

18. Counsel for defendant DADYAN has not responded to the government's proposed stipulation and protective order.

19. In the interests of providing fulsome discovery to defendants in a timely fashion, the government has thus prepared and filed this ex parte application requesting a protective order that will permit the government to produce discovery with minimal redactions, but preserves the privacy and security of third-parties and protects the public in general by preventing the defendants from accessing sensitive information outside of their respective defense teams' presence.

20. On December 7, 2020, the government notified counsel for each defendant via email that it intended to file the instant ex parte application, and requested they advise the government whether they oppose the ex parte nature of this application. Counsel for defendant TERABELIAN, A. AYVAZYAN, and DADYAN have not yet responded to the government's email. At approximately 5:02 p.m. on December 7, 2020, counsel for defendant R. AYVAZYAN responded via email that defendant R. AYVAZYAN would be filing at 5:05 p.m. his own ex parte application to compel production of discovery in this matter.

21. In light of concerns raised by counsel for defendants R. AYVAZYAN and TERABELIAN regarding the potential impact of COVID-19 on trial preparations, the government has added a paragraph (paragraph 13.m above) to the proposed order filed concurrently herewith to indicate that the defense teams may use video conferencing systems, such as Zoom, WebEx, Microsoft Teams, or Blue Jeans, to review Confidential Information with defendants or witnesses, provided that counsel for the defendants certifies in writing that there is no way for defendants or witnesses to maintain electronic copies of the Confidential Information once the video conference is over. The government has also added a paragraph to the protective order (paragraph 13.b above) in order to clarify that the protective order applies to counterfeit and unauthorized access devices, which materials may not have been fully covered under the protective order the government originally sent to defendants' counsel on November 30, 2020.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that

this declaration is executed at Los Angeles, California, on December 7, 2020.

/s/

JULIAN L. ANDRÉ