TRACY L. WILKISON
Acting United States Attorney
BRANDON D. FOX
Assistant United States Attorney
Chief, Criminal Division
SCOTT PAETTY (Cal. Bar No. 274719)
BRIAN FAERSTEIN (Cal. Bar No. 274850)
Assistant United States Attorneys
Major Frauds/Environmental and Community Safety Crimes Sections
1100/1300 United States Courthouse
312 North Spring Street
Los Angeles, California 90012
Telephone: (213) 894-6527/3819
Facsimile: (213) 894-6269/0141
E-mail: Scott.Paetty@usdoj.gov/Brian.Faerstein@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) 320-0539
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, MANUK GRIGORYAN, aka “Mike Grigoryan,” and “Anton Kudiumov,” ARMAN HAYRAPETYAN, EDVARD PARONYAN,	No. CR 20-579(A)-SVW <u>GOVERNMENT’S CONSOLIDATED OPPOSITION TO DEFENDANT AYVAZYAN’S AND DEFENDANT TERABELIAN’S MOTIONS TO SUPPRESS (ECF 130, 135, 136); DECLARATIONS OF SCOTT PAETTY AND TIMOTHY MASSINO; EXHIBITS</u>

aka "Edvard Paronian" and "Edward Paronyan," and VAHE DADYAN, Defendants.	Hearing Date: April, 12, 2021[1] Hearing Time: 11:00 a.m. Location: Courtroom of the Hon. Stephen V. Wilson

Plaintiff United States of America, by and through its counsel of record, the Acting United States Attorney for the Central District of California and Assistant United States Attorneys Scott Paetty and Brian Faerstein, and United States Department of Justice Trial Attorney Christopher Fenton, hereby files its Consolidated Opposition to defendant Richard Ayvazyan's and defendant Marietta Terabelian's Motions to Suppress (ECF Nos. 130, 135, 136).

This opposition is based upon the attached memorandum of points and authorities, the Declaration of Scott Paetty and attached

//

//

[11] Defendants noticed a hearing on these motions for April 5, 2021. However, defendant Richard Ayvazyan subsequently filed a separate motion to suppress (ECF 146) and noticed a hearing on that motion for April 12, 2021. To foster the efficient use of the Court's resources, the government respectfully requests that any hearing on these motions be consolidated to the later date, or at a time thereafter that is convenient for the Court.

exhibits, the Declaration of Timothy Massino, the files and records in this case, and such further evidence and argument as the Court may permit.

Dated: March 15, 2021

Respectfully submitted,

TRACY L. WILKISON
Acting United States Attorney

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

/s/
SCOTT PAETTY
BRIAN FAERSTEIN
Assistant United States Attorneys
CHRISTOPHER FENTON
Department of Justice Trial Attorney

Attorneys for Plaintiff
UNITED STATES OF AMERICA

TABLE OF CONTENTS

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES (CONTINUED)

TABLE OF AUTHORITIES (CONTINUED)

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Defendant Richard Ayvazyan ("Ayvazyan") and his wife Marietta Terabelian ("Terabelian") (collectively, "defendants") orchestrated a vast fraud ring that used an array of fake businesses, aliases, and stolen identities, to steal tens of millions of dollars from the Paycheck Protection Program ("PPP") and Economic Injury Disaster Loan Program ("EIDL")---federal loan programs which were intended to assist struggling businesses during the COVID-19 pandemic. Defendants then impermissibly used the disaster relief funds for their own personal use and enjoyment, including to buy luxury homes, gold coins, diamonds, jewelry, luxury watches, fine imported furnishings, designer handbags and clothing, cryptocurrency, and securities.

Defendants now seek to suppress items that were legally seized from them at the airport in Miami, Florida, as they returned to the United States from a luxury vacation in Turks and Caicos, including credit cards in the names of "Iuliia Zhadko" and "Viktoria Kauichko," two fake identities used by defendants to carry out the loan fraud scheme, as well as digital contraband in the form of numerous images of drivers' licenses, personal identification documents, and credit cards in an assortment of names. The border search of defendants, the seizure of physical and digital contraband, the interviews of defendants during the border stop, and the search warrants that were subsequently obtained on the devices and defendants' residence were conducted lawfully and comported with the constitution, and therefore defendants' motions to suppress (ECF 130, 135, 136) should be denied.

II. STATEMENT OF FACTS

A. The Investigation

In June 2020, the government opened an investigation into a Los Angeles-based ring that was using stolen, fake, and synthetic identities to fraudulently apply for COVID-19 relief funds. (Declaration of Timothy Massino ("Massino Decl.") ¶ 1.) The original subjects included "Iuliia Zhadko" (later determined to be a fake identity), who submitted fraudulent loan applications on behalf of Top Quality Contracting and Turing Info Solutions. (Id. ¶ 2.) Among other things, the driver's license submitted in support of Zhadko's applications was fake. (Id. ¶ 3.)

Over the next four months, the government served over 200 subpoenas, obtaining information from federal and state agencies, lenders, retail banks, and escrow companies, among others. (Id. ¶ 4.) The government identified additional fraudulent loan applications, including one using the name "Viktoria Kauichko" (also later identified as fake) submitted on behalf of Runyan Tax Services. (Id. ¶ 5.) The government traced the funds and learned that the proceeds had been funneled through various bank accounts, including one in defendant Terabelian's name, and had been used by her husband, defendant Ayvazyan, to purchase luxury homes, including a $3.25 million mansion that defendants put in their own names. (Id. ¶ 6; ECF 1.) Further investigation revealed that, in 2012, both defendants had pled guilty to conspiracy to commit bank fraud for their role in a similar scheme involving fraudulent loan applications. See United States v. Ayvazyan, et al., 11-cr-180 (CDCA). The government identified them as targets and submitted their names to the Department of Homeland Security ("DHS") TECS System, which provides travel alerts. (Id. ¶ 7.)

B. The Border Stop in Miami International Airport

On October 16, 2020, FBI SA Justin Palmerton received notice that defendant Terabelian was traveling from Turks and Caicos to the United States via the Miami International Airport ("MIA"). He contacted Customs and Border Protection ("CBP") to ask that she be referred for secondary inspection, explaining she may be involved in "the use of stolen/synthetic identities and businesses" and may be "transporting fake id's, gold or large amounts of cash." (See Declaration of Scott Paetty ("Paetty Decl."), Ex. 1.)

On October 19, 2020, at around 3:30 p.m., defendants arrived at MIA and were referred for secondary inspection. CBP Officers conducted a search of defendants' belongings and found (i) in defendant Terabelian's luggage, a credit card in the name of "Viktoria Kauichko"; and (ii) in defendant Ayvazyan's belongings, one credit card in the name of "Runyan Tax Services/Viktoria Kauichko," and four credit cards in the name of "Iuliia Zhadko," including cards associated with "Top Quality Contracting" and "Turing Info Solutions." (Id., Exs. 2, 3.)

CBP Officers also conducted a "basic search" of defendant Terabelian's iPhone and one of defendant Ayvazyan's five digital devices.[1] CBP provided defendants with a copy of the "Inspection of Electronic Devices" tear sheet (Id., Exs. 5, 6), which explained that

[1] CBP defines a "basic search" as a manual search, without the aid of external equipment, that may be conducted with or without suspicion. (Paetty Decl.; Ex. 4 at § 5.1.3.) An "advanced search" involves the use of external equipment to conduct a forensic analysis of the contents of a digital device. (See id. at § 5.1.4.)

CBP had authority to search defendants' digital devices and that, if they did not provide passcodes, their digital devices could be detained for inspection and returned at a later date (Id.; Ex. 7.) Defendants both provided passcodes. (Id., Exs. 5, 6.) CBP Officers notified their supervisors and documented the search. (Id.) The basic search of defendants' digital devices revealed digital photographs of a driver's license in the name of "Iuliia Zhadko" with defendants' home address, a social security card in Zhadko's name, and numerous other credit cards and driver's licenses in various names. (Id., Ex. 8.)

As part of the secondary inspection process, CBP Officers interviewed defendants, including about information they provided on a biographical questionnaire. (Id., Ex. 9.) The interviews were memorialized in written reports and some portions were also video recorded. (Id., Exs. 5, 6.)[2]

C. Defendants' Arrest and Subsequent Search Warrants

On October 20, 2020, at around 1:45 a.m., CBP admitted defendants and turned them over to the FBI, who made a probable cause arrest. (Id., Ex. 10.) Later that day, the government filed a complaint against defendants, alleging conspiracy to commit bank and wire fraud. (ECF 1.) The government subsequently obtained warrants to search the six digital devices seized incident to defendants' arrest and seven premises (including two of defendants' homes). The basis for probable cause included volumes of evidence independent of

[2] The government made a good faith effort to produce a copy of all video and audio recordings made of the interviews. Approximately four hours of recordings was produced. Other video recordings of the interviews may have been inadvertently deleted and subsequent efforts to recover them have been unsuccessful. (Paetty Decl., Ex. 14.)

the border stop, such as loan applications and bank records, surveillance, and trash pulls. (See, e.g., Id. Ex. 11 (20-mj-5282), Ex. 12 (20-mj-5484).)

D. Indictment and First Superseding Indictment

On November 17, 2020, a grand jury indicted the defendants and two others with, among other charges, conspiracy, bank fraud, and wire fraud, based on 35 fraudulent loan applications seeking over $5.6 million in COVID-19 relief funds. (ECF 32.) On March 9, 2021, a grand jury returned a superseding indictment that significantly expanded the charges. In addition to naming four new defendants, the superseding indictment charges the original defendants with conspiracy to commit money laundering and aggravated identity theft. It also charges defendant Ayvazyan with new crimes he committed while on pretrial release. As alleged, the scheme involves at least 151 fraudulent loan applications seeking over $21.9 million in COVID-19 relief funds.

III. ARGUMENT

A. The Searches and Seizures at Miami International Airport were Valid Exercises of the Government's Border Search Authority

Goods and property crossing international borders are not subject to ordinary warrant requirements. Rather, the government's "inherent sovereign authority to protect its territorial integrity" itself demonstrates the reasonableness of a border search. Torres v. Commonwealth of P.R., 442 U.S. 465, 472–73 (1979). "[B]order searches typically do not require any particularized suspicion, so long as they are routine inspections and searches of individuals or conveyances seeking to cross our borders." United States v. Cano, 934 F.3d 1002, 1012 (9th Cir. 2019). "Such searches are reasonable simply by virtue of the fact they occur at the border." Id.

The border search and seizures that are the subject of defendants' motions to suppress fell squarely within this longstanding exception to the warrant requirement. Upon learning through TECS that defendants would be arriving at MIA from Turks and Caicos, FBI SA Palmerton sent CBP an email alerting customs officials that defendants may be "transporting fake id's" related to suspected fraudulent loan applications involving "stolen/synthetic identities and businesses." (Paetty Decl., Ex. 1.) CBP thereafter conducted a secondary inspection of defendants pursuant to its border search authority. During the search, CBP found both physical credit cards in fake names and digital contraband reflecting counterfeit identification documents and credit cards on defendants' phones.

Defendant Ayvazyan principally challenges the legitimacy of the border search on the basis that it was "pretextual" and "conducted under the authority and direction of the FBI, not CBP." (ECF 130 at 15-18.) Defendant's arguments fail as a matter of law and practice.

First, the fact that the FBI referred the matter to CBP does not undermine the validity of the border search. Courts have consistently rejected challenges to border searches where the customs officers who conducted them collaborated with other law enforcement agencies. The Ninth Circuit rejected this very argument in Cano, explaining, "[w]e have upheld border searches of persons seeking entry even when those searches were conducted 'at the behest' of DEA agents seeking criminal evidence." Cano, 934 F.3d at 1016 n.9; see also United States v. Schoor, 597 F.2d 1303, 1306 (9th Cir. 1979) ("Here there is no dispute that the search was conducted at an international border by customs officers legally entitled to search persons entering the United States. That the search was made at the request of the DEA officers does not detract from its legitimacy.”); United States v. Levy, 803 F.3d 120, 123 (2d Cir. 2015) (“Official interagency collaboration, even (and perhaps especially) at the border, is to be commended, not condemned.”). Not only is such coordination between federal law enforcement unsurprising, but it falls squarely within CBP’s role as the gatekeeper at and protector of the U.S. border. The border search authority is essential to the ability of DHS and CBP to fulfill statutory responsibilities, including to “ensure the interdiction of persons and goods illegally entering or exiting the United States”. 6 U.S.C. §§ 202, 211.

Second, as a practical matter, TECS hits that provide a predicate for secondary screenings at the border are common and entirely permissible so long as the search is conducted by CBP (or other officials with border authority) and the search focuses on the interdiction of contraband. See, e.g., United States v. Cotterman, 709 F.3d 952 (9th Cir. 2013) (reversing suppression after CBP search found digital contraband pursuant to a TEC hit); United States v. Hassanshahi, 75 F. Supp. 3d 101, 117 (D.D.C. 2014) (denying suppression after CBP found incriminating evidence based on a TECS hit).

Defendants’ additional pretext arguments relating to terrorism (ECF 130 at 16-17; ECF 136 at 10-11), are inapposite because, here, the TECS hit and FBI referral expressly discussed defendants’ nexus to fake identification documents and the need for CBP to initiate a secondary screening to prevent such contraband from entering the United States. Cano, 934 F.3d at 1013–14 (“the purpose of the border search is to interdict contraband"). This legitimate rationale for conducting a secondary stop proved prescient: CBP found fake credit cards and digital photographs of fake identification documents and credit cards, all pursuant to its legitimate exercise of its border search authority.

1. The Seizure of Credit Cards in the Names of Iuliia Zhadko and Viktoria Kauichko was Justified

During its search of defendant's luggage and personal belongings, CBP found credit cards not in defendants' names but rather in the names of defendants' suspected fake aliases, "Iuliia Zhadko" and "Viktoria Kauichko." The search of defendants' belongings and seizure of these items was proper under the government's plenary border search authority. Suspicionless border searches have been endorsed in an array of contexts, including searches of "(1) the contents of a traveler's briefcase and luggage; (2) a traveler's 'purse, wallet, or pockets'; (3) papers found in containers such as pockets; and (4) pictures, films and other graphic materials." United States v. Arnold, 533 F.3d 1003, 1007 (9th Cir. 2008) (internal citations omitted).

Credit cards, which are "access devices" under 18 U.S.C. § 1029(e)(1), in the names of fake identities constitute contraband subject to seizure under the border search exception. Indeed, there can be no legitimate purpose for the possession, use, or transfer of such counterfeit access devices.[3] See generally 18 U.S.C. § 1029(a). Contrary to defendant Ayvazyan's contentions regarding the purpose of

---

[3] 18 U.S.C. § 1029(e)(2) defines "counterfeit access device" to mean "any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device."

the border search (ECF 130 at 17), CBP had a legitimate basis in seizing these counterfeit access devices as contraband in furtherance of "enforce[ing] importation laws, and not for general law enforcement purposes." Cano, 934 F.3d at 1013 (internal quotations omitted). Thus, defendants' challenge to the seizure of these physical contraband items should be rejected.

2. The Manual Search of Defendants' Digital Devices and Seizure of Digital Contraband was Justified

During the secondary screening, CBP agents also conducted a routine, manual search of defendants' digital devices that resulted in the lawful seizure of digital contraband, including photographs of counterfeit access devices and identification documents.[4]

In Cano, the Ninth Circuit held that "[m]annual searches of a cell phone at the border can be conducted without any suspicion whatsoever." Cano, 934 F.3d at 1019. The court further explained that, in conducting a manual suspicionless search or a forensic search supported by reasonable suspicion, "border officials are limited to searching for contraband only."[5] Id. The court posited that the "best example" of "digital contraband" is child pornography, but it did not limit the definition to this specific category of contraband. Id. at 1014.

---

[4] These items included a photograph of a fake driver's license in the name of "Iuliia Zhadko" with an address matching defendants' actual home address and featured a photograph of a man resembling defendant Ayvazyan, as well as numerous other photographs of driver's licenses and credit cards in the names of various individuals. (See Paetty Decl., Exs. 5, 6, 8.)

[5] CBP's search of defendants' digital devices here was a manual, not a forensic, search. In any event, based on the initial referral email from FBI, CBP had, at a minimum, reasonable suspicion to conduct a forensic search of defendants' phones for contraband at the time of the search.

The digital photographs of counterfeit access devices, identification documents, and means of identification found during CBP's manual search here constitute another such form of digital contraband. Indeed, an item is contraband per se "if its possession, without more, constitutes a crime; or in other words, if there is no legal purpose to which the object could be put." United States v. Harrell, 530 F.3d 1051, 1057 (9th Cir. 2008). For example, in United States v. Bolar, the Ninth Circuit held that photographic negatives of Federal Reserve Notes are contraband per se because "there is no legal purpose to which those negatives could be put." 569 F.2d 1071, 1072 (9th Cir. 1978).[6]

The photographs of counterfeit credit cards and identification documents on defendants' phones here pose the same core concerns recognized in Cano with respect to the illegal possession, use, and transfer of digital contraband, such as child pornography. "The contents may be digital when they are on the phone, but the physicality of the phone itself and the possibility that the phone's contents can be printed or shared electronically gives border officials sufficient reason to inspect it at the border." Id. at 1013–14. Indeed, fake drivers' licenses and counterfeit credit cards, and the information contained on their face, are illicit commodities that are bought, sold, and transferred among fraudsters to execute their criminal schemes. As alleged in the first

[6] Notably, while citing Bolar, a court in this district ruled that fake California drivers' licenses constituted contraband. See Santos-Pineda v. Axel, No. CV 10-6285 MMM, 2011 WL 13103995, at *7 (C.D. Cal. July 26, 2011), aff'd, 621 F. App'x 407 (9th Cir. 2015) (citing Sash v. United States, No. 09 Civ. 450, 2009 WL 3007379, *3-4 (S.D.N.Y. Sept. 22, 2009) ("[defendant] was convicted of unlawful transfer of badges and ID cards . . . The badges and identifications themselves are contraband per se")).

superseding indictment in this case, the fake identities and corresponding identification documents of Iuliia Zhadko and Viktoria Kauichko were, in fact, used by defendants in submitting fraudulent PPP and EIDL loan applications and opening bank accounts, among other things. The photographs of the counterfeit access devices and identification documents, and the underlying fake means of identification, found on defendants' phones and seized by CBP have no legitimate purpose and exist only to further criminal activity.

Defendant Terabelian incorrectly alleges that forensic searches were conducted on the digital devices. (ECF 136 at 12-13.) As reflected in CBP reports, however, a basic manual, not forensic, search was conducted on all devices. (See Paetty Decl., Ex. 5 at 3; Ex. 6 at 4.) Defendant Ayvazyan similarly challenges the searches of the digital devices as being unreasonable due to the length of time CBP possessed the devices. (ECF 130 at 19-21.) The fact that the manual searches of defendants' digital devices took place over several hours is not, in and of itself, unreasonable. Electronic devices can contain immense amounts of data and are capable of storing contraband that could be located in unexpected places on a phone. See, e.g., Cano, 934 F.3d at 1019 ("Criminals may hide contraband in unexpected places, so it was reasonable for the two HSI officers to open the phone's call log to verify that the log contained a list of phone numbers and not surreptitious images or videos."). Even if a more advanced forensic search had been conducted (which it was not), such a search would have been supported by reasonable suspicion based on the TECS hit and referral of information provided by FBI to CBP.

Defendants also contend that they did not give valid consent to the officers to use their passcodes to access the digital devices. (ECF 130 at 21-23; ECF 136 at 13-15.) This argument is irrelevant because, as discussed above, CBP has the right and ability to conduct a basic search of all digital devices for contraband regardless of whether consent is provided. (See Paetty Decl., Ex. 4 at §§ 5.3.3, 5.3.4.) Indeed, CBP is authorized to request passcodes for any encrypted digital devices at the border and, if passcodes are not provided, to detain the devices for further review pending determination of the devices admissibility. (Id. at § 5.3.1).

These facts were communicated to defendants during the secondary inspection. They were given a copy of a CBP "Inspection of Digital Devices" tear sheet describing the scope of CBP's authority to review their devices and defining defendants' rights in that process. (Id., Ex. 7; Ex. 5 at 3; Ex. 6 at 4.) Defendants' challenge to the basis for their consent is irrelevant. CBP was authorized to manually search the devices at the border — with or without defendants' consent. Neither case defendants cite in support of their consent arguments address border searches. (ECF 130 at 21 (citing United States v. Reid, 226 F.3d 1020 (9th Cir. 2000); ECF 136 at 14 (citing United States v. Ocheltree, 622 F.2d 992 (9th Cir. 1980)).

Moreover, the CBP tear sheet also explained to defendants that they may be subject to inspection because "you have a name that matches a person of interest in one of the government's enforcement databases; or you have been selected for a random search," and further advised them that "CBP officers may not be able to answer all of your questions about an examination that is underway." (Paetty Decl., Ex. 7 at 2.) That CBP officers may have told defendants that they were randomly selected or selected to ensure they were not affiliated with terrorists, as opposed to being the subject of a TECS hit, does not matter. There is no requirement that the officers disclose to defendants that the TECS hit was the actual reason for the stop. Accordingly, CBP's manual search of defendants' digital devices and seizure of digital contraband pursuant to its border search authority was justified in this case.[7]

B. The Good Faith Exception Applies to the Manual Search of the Digital Devices in Miami Consistent With Controlling Eleventh Circuit Precedent

As discussed above, CBP's manual searches of defendants' digital devices (in addition to the physical search of their possessions) were constitutional and comported with Ninth Circuit authority. But even if the Court disagrees, CBP's searches should be subject to the good faith exception to the exclusionary rule.

Recognizing that "[e]xclusion exacts a heavy toll on both the judicial system and society at large," the Supreme Court has established that the exclusionary rule does not apply "when the police conduct a search in objectively reasonable reliance on binding judicial precedent." Davis v. United States, 564 U.S. 229, 237-27, 249-50 (2011). "An officer who conducts a search in reliance on binding appellate precedent does no more than ac[t] as a reasonable officer would and should act under the circumstances." Id. at 241 (internal quotations omitted).

---

[7] To the extent any of the digital information seized pursuant to the manual searches of defendants' digital devices constituted evidence of criminal conduct but not digital contraband, such evidence was independently obtained through the execution of a subsequent warrant to search all six of defendants' digital devices. See infra section III.C.

The manual search of defendants' digital devices occurred in Miami, Florida, and thus the relevant question is whether binding Eleventh Circuit precedent authorized the border search of the devices. As one district court explained,

> tainted evidence obtained within [a different circuit] but nonetheless admissible there should also be admissible here regardless of whether this circuit has a more stringent exclusionary device. Applying the principles that form the foundation of the Court's lex loci approach, the Court finds that there is no logical basis for the conclusion that the forum should reward or punish the Government with either a more lenient or a more severe penalty than that proclaimed by the courts of the jurisdiction where the conduct occurred.

United States v. Gerena, 667 F. Supp. 911, 927 (D. Conn. 1987). Numerous other district courts have similarly held that where, as here, a court in one circuit is considering the propriety of law enforcement's actions in another circuit, the court should apply the law of the circuit where the challenged conduct occurred, i.e., the "lex loci" of the conduct. See, e.g., United States v. Kennedy, No. CR 13-240, 2014 WL 6090409, at *5 (W.D. Pa. Nov. 13, 2014) (Sixth Circuit law applied to search and seizure that occurred in Sixth Circuit but was challenged in Third Circuit); United States v. Gates, No. CR 08-42-P-H, 2008 WL 5382285, at *7 (D. Me. Dec. 19, 2008), aff'd, 709 F.3d 58 (1st Cir. 2013) (Fourth Circuit law applied in First Circuit); United States v. Barragan, 589 F. Supp. 2d 1012, 1015–16 (S.D. Ind. 2008) (Ninth Circuit law applied in Seventh Circuit). These courts have generally reasoned that officers should be able to rely on their understanding of the law as their circuit has interpreted it. See generally id.

The Eleventh Circuit has not adopted Cano's framework for searching digital devices at the border, nor has it distinguished between the government's ability to conduct a manual search for digital contraband or evidence of criminality. However, the court has expressly rejected the Ninth Circuit's limited view of border search authority as articulated in United States v. Cotterman, 709 F.3d 952 (9th 2013) – a case significantly relied on by the panel in Cano. See United States v. Touset, 890 F.3d 1227 (11th Cir. 2018).

In Touset, the Eleventh Circuit held that customs officials did not need to have reasonable suspicion in order to conduct a forensic (as opposed to a manual) search of a cell phone. Id. at 1233. In so holding, the court carefully considered the Ninth Circuit's reasoning in Cotterman, concluding that it was "unpersuaded" and "fail[ed] to see how the personal nature of data stored on electronic devices could trigger" a greater "personal indignity" than a suspicionless search of a home at the border. Id. at 1234. Moreover, the Touset court also found that Riley v. California, 573 U.S. 373 (2014) (also a case Cano relies on to narrow the scope of the border search), 934 F.3d at 1011, 1020, has no application at the border. See 890 F.3d at 1234. In sum, the Eleventh Circuit has firmly rejected significant tenets underlying the Cano panel's more narrow view of the government's border search authority of digital devices.

In conducting the manual searches of the digital devices at issue here, the CBP officers in Miami relied upon "binding judicial precedent" within the Eleventh Circuit and acted as "a reasonable officer would and should act under the circumstances." Davis, 564 U.S. at 239, 241. Thus, should the Court find that CBP's searches of the digital devices or seizures of digital contraband violated Ninth Circuit border search precedent, the Court should nonetheless find that CBP's actions fall squarely within the good faith exception.

See Davis, 564 U.S. at 241 ("About all that exclusion would deter in this case is conscientious police work.").

C. The Government Obtained Valid Warrants to Search the Digital Devices Seized from Defendants in Miami and to Search Defendants' and Co-conspirators' Residences

Defendant Ayvazyan also summarily challenges subsequent search warrants obtained by the government as the purported "fruit of the poisonous tree" of the border search at issue in his motion. (ECF 130 at 24; ECF 135 at 18.) Defendant Ayvazyan ignores the extensive investigation that preceded the border search in October 2020, as well as the actual content of the affidavits in support of these warrants, which were based substantially on evidence independent of the border stop. The exclusionary rule is not appropriate under these circumstances.

"Exclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment." Davis, 564 U.S. at 237 (internal citations omitted). Suppression thus is a remedy of "last resort." Id. Application of the exclusionary rule is "particularly" inappropriate when "an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." United States v. Leon, 468 U.S. 897, 920 (1984). "In most such cases, there is no police illegality and thus nothing to deter." Id. at 920-21. Once a judge signs a warrant, "there is literally nothing more the policeman can do in seeking to comply with the law." Id. at 921.

The warrants at issue here were lawfully obtained and largely independent of information developed during the border stop. In particular, around two weeks after the border stop, agents obtained warrants to search seven residences linked to the scheme and to search the original defendants charged in this case. (See Paetty Decl., Ex. 11.)[8] Shortly thereafter, the government obtained a search warrant for the six digital devices seized in Miami.[9] (See id., Ex. 12.)

The warrants resulted in the seizure of, among other things, additional evidence corroborating defendants' use of their aliases, Iuliia Zhadko and Viktoria Kauichko, to apply for fraudulent PPP and EIDL loans. The warrants also yielded evidence connecting defendants' coconspirators to the scheme, such as stolen stamping devices from notaries and clerks of court (including a stamp from the clerk of the Bankruptcy Court for the Central District of California). (See id., Ex. 13 at 1.)

In establishing probable cause, the affidavits in support of the search warrants for the residences and individuals relied in substantial part on evidence obtained during the months-long investigation that preceded the border search in Miami. Indeed, by the time of the border stop in October 2020, federal agents had been investigating defendants' fraudulent loan scheme for more than four

[8] The government submitted the same central affidavit in support of the eleven search warrant applications. We attach one application here – an application for the search of defendants' residence located at 4910 Topeka Drive in Tarzana – as an exact representation of the probable cause statement supporting the other ten applications.

[9] The warrants, which remain under seal, have the following case numbers: 20-MJ-5282, 20-MJ-5284, 20-MJ-5285, 20-MJ-5286, 20-MJ-5288, 20-MJ-5289, and 20-MJ-5290 (for the seven residences); 20-MJ-5292, 20-MJ-5293, 20-MJ-5294, and 20-MJ-5296 (for the four defendants); and 20-MJ-5484 (for the six digital devices).

months. During that time, agents had conducted numerous interviews, pursued leads and other investigative activities, obtained information from federal and state agencies, lenders, banks, and other entities, and served more than 200 grand jury subpoenas. (See Massino Decl. ¶ 4.) The statements of probable cause supporting the search warrant applications for the residences and individuals were based predominantly on the fruits of this independent investigation, not the more limited information derived from the border search in Miami. (See generally Paetty Decl., Ex. 11.) The affidavit in support of the subsequent devices search warrant application directly incorporated and attached the probable cause statement from these prior search warrants, as well as the affidavits in support of the criminal complaints filed against all four original defendants, which also detailed the investigation preceding the border stop. (See generally id., Ex. 12.). In short, all of the search warrant applications were supported in substantial part by significant evidence of probable cause obtained independent of the border stop in Miami.

Moreover, even if the border search resulted in illegally obtained evidence (which it did not), the isolated references to such evidence in the search warrant affidavits do not invalidate the entire warrants. "[T]he mere inclusion of tainted evidence in an affidavit does not, by itself, taint the warrant or the evidence seized pursuant to the warrant." United States v. Vasey, 834 F.2d 782, 788 (9th Cir. 1987). "A reviewing court should excise the tainted evidence and determine whether the remaining, untainted evidence would provide a neutral magistrate with probable cause to issue a warrant." Id. This is so because a "warrant may be upheld even where it contains tainted and untainted facts as long as the untainted portions contain a sufficient showing of probable cause to render the warrant valid." United States v. Driver, 776 F.2d 807, 812 (9th Cir. 1985). In reviewing information in support of a search warrant, courts should do so in a "common sense and realistic fashion." Id. at 811.

In light of the ample evidence detailed in the warrant applications linking defendants to the fraud scheme independent of the Miami border stop, the subsequent search of the defendants, the subject residences, and defendants' digital devices pursuant to those warrants was not unreasonable at all, much less "obviously" unreasonable. Messerschmidt v. Millender, 565 U.S. 535, 556 (2012) (the question under the good-faith exception is not whether the magistrate judge "erred" in issuing a warrant, but whether "the magistrate so obviously erred that any reasonable officer would have recognized the error"). The warrants were obtained primarily independent of any purported Fourth Amendment violations from the border stop, and evidence obtained from these warrants should not be excluded.

D. Defendants Were Not Entitled to Miranda Warnings Prior to Secondary Screening

Defendants also seek to suppress statements they made during secondary screening, contending that the questioning violated their constitutional rights because they were not given Miranda warnings. (ECF 135 at 11-18; ECF 136 at 6-12.) Defendants' Fifth Amendment and Sixth Amendment challenges should be rejected as well.

As a threshold matter, the government does not dispute that video evidence relating to portions of the interviews conducted by

CBP officers may have been inadvertently deleted by CBP despite the government's good faith efforts to preserve such information. However, to the extent it existed and was deleted, such video evidence would be, at most, relevant only to defendants' motions to suppress statements made during the video recorded interviews. Such evidence would not be relevant to the seizure of the physical contraband from defendants' personal belongings or CBP's basic search of defendants' digital devices (which did not require consent or even the passcodes). Defendants' other arguments – about the alleged denial of the right to counsel and about the alleged tactics used by CBP during the interviews – are similarly relevant only to defendants' motion to suppress statements. Importantly, defendants do not actually identify any statements that they made during these interviews that should be suppressed. But even if they did and the Court were to find suppression to be warranted, the proper remedy would be to suppress those statements only.

Defendants' allegations that the government acted in bad faith are directly refuted by the government's transparency in detailing for counsel and the Court the information it learned about the secondary stop, including about the video evidence that may have been inadvertently deleted, and the extensive efforts undertaken by CBP to recover such evidence. (See Paetty Decl., Ex. 14.) Defendants' allegations of bad faith are further undermined by the fantastical nature of their alleged motive, a purported government cover-up of the use of policies and procedures that are public knowledge (such as interagency coordination among federal law enforcement agencies, the use of the TECS System in secondary inspections, and search of digital devices at the border). Not only has the federal government made such information available to the general public (see, e.g., https://www.dhs.gov/publication/tecs-system-cbp-primary-and-secondary-processing-tecs-national-sar-initiative), but it provides certain information – such as about the search of digital devices at the border – directly to travelers, like defendants, in mass-produced handouts. (See Paetty Decl., Exs. 4, 7.)

In any event, questions at the border do not trigger Miranda merely because they are posed during a secondary screening at the border. United States v. Kiam, 432 F.3d 524 (3d Cir. 2006). Courts agree that such questioning can also be viewed as non-custodial, even if the individual is not free to leave. See, e.g., United States v. Fernandez-Ventura, 132 F.3d 844, 846 (1st Cir. 1998); United States v. FNU LNU, 653 F.3d 144 (2d Cir. 2011); United States v. Bengivenga, 845 F.2d 593, 599 (5th Cir. 1988) (en banc); United States v. Galloway, 316 F.3d 624 (6th Cir. 2003); United States v. Gupta, 183 F.3d 615 (7th Cir. 1999); United States v. Moya, 74 F.3d 1117, 1120 (11th Cir. 1996).

For the reasons explained above in section III.B with respect to digital devices, under the "lex loci" approach, the law of the Eleventh Circuit should apply. In Moya, the Eleventh Circuit held that because of the sovereign's responsibility to secure its borders, "some degree of questioning and of delay is necessary and is to be expected at entry points into the United States." 74 F.3d at 1120. "Because of this expectation, questioning at the border must rise to a distinctly accusatory level before it can be said that a reasonable person would feel restraints on his ability to roam to the degree associated with formal arrest." Id. (internal quotations omitted). Events which might be enough often to signal "custody" away from the border will not be enough to establish "custody" in the context of entry into the country. Id. In sum, Miranda warnings are not required under these circumstances even in cases where a secondary interview is part of the border routine. Id.

But even if the Court applies Ninth Circuit law, questioning at the border similarly is afforded more latitude. See United States v. Guzman-Padilla, 573 F.3d 865, 883-84 (9th Cir. 2009) (noting that the Government has more leeway to detain individuals at the border without effecting an arrest because "special rules apply at the border"); see also United States v. Nava, 363 F.3d 942, 946 (9th Cir. 2004) (defendant not arrested at border after being escorted in handcuffs to security office, having pat down search conducted, and being forced to wait in locked office during truck search).

Defendants were being interviewed to determine their admissibility into the United States. Under 8 U.S.C. § 1225(a)(5), CBP officers may require any applicant for admission into the United States to give statements to assist the officers in determining whether the applicant is admissible. In addition, the Ninth Circuit recognizes that under 19 U.S.C. § 1582, all persons entering the United States are subject to search and detention, including to answer "routinely asked questions" regarding, among other things, their travels and "any merchandise or goods" they are carrying with them. United States v. Chavez-Martinez, 407 F.2d 535, 539 (9th Cir. 1969); see also United States v. Reyes, 631 F.2d 616, 622 (9th Cir. 1980) ("[R]outine inquiries during extended border searches concerning ownership of the containers crossing the border do not constitute 'custodial interrogation' within the meaning of Miranda."); United States v. Ozuna, 170 F.3d 654, 658 (6th Cir. 1999)

("Other courts have held consistently that the Miranda warnings need not precede initial routine questioning by Immigration or Customs officials because such questioning is not 'custodial interrogation'").

Notably, defendants do not actually identify any statements they made that they seek to suppress. The practical effect of defendants' motion to suppress these unidentified statements is therefore to put before the Court defendants' version of events, which, according to them, include their repeated efforts to invoke a right to counsel. There are, however, significant reasons to question defendants' credibility. Defendants both previously pled guilty for their joint participation in a conspiracy to commit bank fraud that included making false and misleading statements about the true identity of defendant Ayvazyan's mother. See United States v. Richard Ayvazyan, CR 11-180-CJC. Moreover, in the declaration he submitted in support of the instant motions, defendant Ayvazyan brazenly lies to this Court when he misrepresents that he had the permission of Viktoria Kauichko and Iuliia Zhadko – who are fake and synthetic identities – to use credit cards opened in their names and omits that he also possessed images of driver's licenses and credit cards in the names of several other individuals. (Ayvazyan Decl. ¶ 22.)

Even accepting defendants' version of events, their description of what they were asked by CBP does not rise to the level of interrogation that would merit Miranda warnings or trigger the need for an attorney, especially at the border. Nor do the alleged categories of questions constitute interrogation about a particular crime – namely, wire or bank fraud involving PPP or EIDL loan funds.

Specifically, according to defendant Ayvazyan, at his secondary inspection he was asked questions about "where [he] was coming from, phone numbers, relatives' names, children's names, social media accounts, employment, bank accounts, whether [he] was associated with organized crime, and whether [he] had any prior convictions" as well as questions about where he lived and his employment. (Ayvazyan Decl. ¶ 17.) Ayvazyan also stated that he was asked whether he owned the digital devices he was carrying and was asked questions about the credit cards he was carrying in the names of Iuliia Zhadko and Viktoria Kauichko. (Id. ¶¶ 18, 22.) According to defendant Terabelian, she was asked questions about her background, her husband, his work, and where she had traveled. (Terabelian Decl. ¶ 16.)

The questions posed to both defendants address either background questions that speak to their identity or questions related to the contraband they carried and as such fall squarely within the realm of routine customs questions required for CBP to fulfill its essential tasks of ensuring that defendants are admissible and interdicting contraband. See Reyes, 631 F.2d at 622. Even accepting defendants' declarations as true, none of the questions purportedly asked by CBP sought information about PPP or EIDL loans, which comports with the scope of questions that SA Palmerton requested that CBP ask defendants. (See Paetty Decl., Ex. 1.) All of these questions are routine customs-related inquiries as reflected on the checklist provided to CBP officers to assist in secondary screenings. (Id., Ex. 9.)

Thus, defendants' own declarations belie their claim that CBP officers asked them questions designed to incriminate them and ultimately undercut the notion that the questions "went to the heart" of the PPP/EIDL loan fraud scheme. (ECF 136 at 7.) Furthermore, the CBP Officers' lack of knowledge of the nature of the charges under investigation (id. at 10) further supports the inference that the officers were not even equipped to interrogate defendants about the loan fraud scheme. And defendant Terabelian's lack of knowledge about what charges she may have faced supports that CBP officers did not ask her questions about those charges or else she would have known what the charges were. (Id.)

Defendants' assertions that they were subjected to an unreasonably lengthy detention are undermined by the fact that they were carrying numerous digital devices that, upon manual review, revealed a trove of digital contraband. As reflected in defendant Terabelian's motion (ECF 136 at 10), defendants also gave inconsistent and conflicting answers to officers' questions and were travelling with credit cards in other people's names. See e.g., Ozuna, 170 F.3d at 658 ("incomplete and inconsistent answers . . . necessitated repetition of the questions."). All of these red flags make it entirely reasonable that defendants would be detained while officers made a determination, pursuant to their plenary authority as gatekeepers at the border, to interdict contraband and ensure that persons seeking admission to the United States were in fact admissible.

IV. CONCLUSION

For the foregoing reasons, the government respectfully requests that this Court deny defendants' motions to suppress.