UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

CASE NO. 23-60019-CR-SINGHAL

UNITED STATES OF AMERICA

vs.

KERVENS SAINT-HILAIRE,

Defendant.
_____/

FACTUAL PROFFER

The United States of America (the "United States") and Defendant Kervens Saint-Hilaire ("Defendant") agree that, were this case to proceed to trial, the United States would prove beyond a reasonable doubt the following facts, among others, which occurred in the Southern District of Florida and elsewhere:

INTRODUCTION

1. From at least October 2019, and continuing through May 2021, Defendant conspired and agreed with co-defendant Patrick Ductant ("Ductant"), co-defendant Vladimir Saint-Hilaire ("Vladimir"), co-defendant Terri Shana Davis ("Davis"), Co-Conspirator 1, and others, to commit bank fraud and wire fraud. The purpose of the conspiracy was for Defendant and his co-conspirators to unlawfully enrich themselves by devising and executing a scheme and artifice to defraud financial institutions and the U.S. Small Business Administration ("SBA"). Defendant knew the unlawful purpose of the plan and willfully joined in it.

2. The bank fraud object of the conspiracy involved, among other things, Defendant and his co-conspirators unlawfully using the means of identification of other persons, and otherwise making materially false and fraudulent representations, to obtain money, funds, credits,

and assets under the custody and control of financial institutions whose accounts were insured by the Federal Deposit Insurance Corporation, including, but not limited to, USAA Federal Savings Bank (hereinafter, "USAA Bank"), Citibank, N.A. (hereinafter, "Citibank"), and TD Bank USA, N.A. (hereinafter, "TD Bank"). The wire fraud object of the conspiracy involved, among other things, Defendant and his co-conspirators unlawfully using the means of identification of other persons, and otherwise making materially false and fraudulent representations, to obtain loans through the SBA's Paycheck Protection Program ("PPP") and Economic Injury Disaster Loan ("EIDL") program. The PPP and EIDL program were designed to provide emergency financial assistance to the millions of Americans who were suffering from the economic effects caused by the COVID-19 pandemic.

3. To carry out the conspiracy and accomplish its purpose, Defendant and his co-conspirators unlawfully acquired personally identifiable information ("PII"), including social security numbers, dates of birth, and driver license numbers, of other persons (hereinafter, "Identity Theft Victims"). Some of the Identity Theft Victims were inmates confined in federal and state prisons who played no role in the conspiracy and did not know that Defendant and his co-conspirator had acquired their PII. All inmate victims were interviewed by law enforcement during the investigation, reviewed the fraudulent documents used in the scheme, and provided sworn statements denying any knowledge or involvement in the criminal activity.[1]

4. Once Defendant and his co-conspirators acquired Identity Theft Victims' PII, including counterfeit driver licenses, they used such means of identification in furtherance of the conspiracy to do the following: (a) apply for and obtain fraudulent loans from financial institutions, including personal loans from USAA Bank issued in the names of Identity Theft Victims; (b) apply

[1] Most, if not all, of the inmates did not have the ability to communicate electronically, nor authority to establish or possess any identification, currency, or credit cards, other than their BOP/corrections identification.

for and obtain fraudulent loans from the SBA, including loans through the PPP and EIDL programs issued in the names of Identity Theft Victims; (c) open fraudulent bank accounts at financial institutions in the names of Identity Theft Victims and conduct fraudulent financial transactions within such accounts, including depositing and withdrawing the proceeds of fraudulent loans; (d) fraudulently obtain and use credit cards and debit cards issued by financial institutions in the names of Identity Theft Victims, including the purchase of money orders made payable to Defendant and his co-conspirators; and (e) otherwise divert fraud proceeds obtained in the names of Identity Theft Victims for the use and benefit of Defendant, his co-conspirators, and others, including, but not limited to, purchases of and/or payments toward homes, home improvements, luxury vehicles, and jewelry, and other expenses.

EVIDENCE SUFFICIENT TO PROVE BEYOND A RESONABLE DOUBT THE OFFENSES TO WHICH DEFENDANT HAS AGREEED TO PLEAD GUILTY

5. Admissible evidence that the government would offer at trial to prove beyond a reasonable doubt that Defendant is guilty of conspiracy to commit bank fraud and wire fraud (Count 1) and aggravated identity theft (Count 16), includes, but is not limited to, the following:

I. Unlawful Acquisition of Victim PII from Davis

6. Text message content (including image and video attachments) obtained from a search warrant executed on Defendant's cell phones establishes that co-defendant Davis was one source of PII that Defendant and his co-conspirators used to perpetrate the fraud offenses. The content on Defendant's phones further establishes that Davis obtained the PII through TransUnion's TLOxp database that she accessed through her employment at a company in Atlanta, Georgia, and that Defendant paid Davis $7 per piece of victim PII to via CashApp. The text messages were not exchanged between Defendant and Davis directly, but between Defendant and Co-Conspirator 1 who facilitated the transfer of the PII (via text messages) from Davis to

Defendant. Co-conspirator 1 was saved as a contact in Defendant's phone as "And 1#*" with the phone number ending in 5382.

7. Specifically, text messages between Defendant and Co-Conspirator 1 date-stamped October 28 and 29, 2019, show that Defendant asked Co-Conspirator 1 if the "tlo plug" (a reference to Davis) could provide Kentucky driver licenses numbers. Co-Conspirator 1 responded that she could get "all the info" but for a minimum of 10 people at $7 per person. Defendant asked how long it would take her to get the information, and Co-Conspirator 1 responded, "If she at work she knock the out ASAP once she get the cashapp." Defendant responded, "Ok find out if she working today" and Co-Conspirator 1 responded "She is I just called her to make sure."

8. Next, a series of text messages between Defendant and Co-Conspirator 1 establishes the following:

a) Co-Conspirator 1 sent Defendant instructions for how to pay Davis, including a screenshot of Davis' CashApp user name, which was "Terri" with the $Cashtag "$TShanaD";

b) Defendant sent Co-Conspirator 1 a screen shot showing a CashApp confirmation that Defendant paid $70 to "Terri" with the $Cashtag "$TShanaD";

c) Defendant sent Co-Conspirator 1 the names of the individuals whose PII (including driver license numbers) Defendant wanted; Co-Conspirator 1 then sent these names to Davis; and

d) Davis ran the queries in the TLO database and sent the requested PII to Co-Conspirator 1, which Co-Conspirator 1 forwarded to Defendant in various formats. This included photographs of Davis' computer screen visibly logged into the TLO database as "Terri.Davis" with the requested PII displayed, and screen shots and

screen videos of a separate text message conversation that Co-Conspirator 1 was contemporaneously having with Davis in which Davis was providing the requested PII to Co-Conspirator 1.

9. In addition to this text message content, the government will offer business records obtained through a subpoena to TransUnion showing historical activity of the TLO database for user "Terri.Davis." The records show that the account for user "Terri.Davis" belonged to her employer, and that "Terri.Davis" had run unauthorized queries for the names and social security numbers of the victims whose information was captured in the screenshots sent to Defendant. Moreover, an activity log shows that the date and time of queries run by "Terri.Davis" is aligned with the date and time of the messages transmitting to information from Davis Co-Conspirator 1, and from Co-Conspirator 1 to Defendant.

II. Procurement of Counterfeit Driver Licenses

10. Digital and physical evidence obtained through search warrants establishes that Defendant and his co-conspirators used the PII supplied by Davis (and others) to procure counterfeit driver's licenses, many of which were used to perpetrate the offenses charged in the Indictment. Specifically, images of at least 72 counterfeit driver's licenses were found in the cell phones of Defendant and Ductant, and dozens of physical counterfeit driver's licenses found at the residence of Defendant and his brother, Vladimir, at 500 SW 145th Ave, Apt. 551, Pembroke Pines (hereinafter, the "Pembroke Pines Residence"). Many of these counterfeit driver's licenses were used to apply for fraudulent loans and open fraudulent bank accounts.

11. Additionally, text messages from Defendant's phone show that he obtained counterfeit driver's licenses from unknown co-conspirators "E faces" and "Rob." For example, Defendant texted "E faces" a picture of a black male's face with PII for identity theft victim J.H.

(a federal inmate who is Caucasian) whose PII Defendant obtained through Davis (including, driver license number, issue date, expiration date, date of birth, height, and address). After sending the picture and PII, Defendant asked E faces: "When do you think you will be finished with it?" E faces responded: "In the am." A subsequent text message conversation between Defendant and Ductant contained an image of a counterfeit Florida Driver License for Identity Theft Victim "J.H." with the PII that Defendant had sent to E faces. Victim J.H.'s PII was used to obtain a $39,500 fraudulent USAA loan and open bank accounts in his name to launder and withdraw the fraud proceeds (during the period in which J.H. was incarcerated).

III. Fraudulent Bank Account Creation and USAA Loan Procurement

12. Tangible, digital, and documentary evidence will prove that Defendant and his co-conspirators created unauthorized bank accounts, procured fraudulent bank loans, and deposited fraudulently obtained loan proceeds into the unauthorized accounts, among other criminal activity.

13. With respect to tangible evidence, the government will introduce evidence obtained from the execution of search warrants at two locations: 1) Defendant's Pembroke Pines Residence; and 2) the office space that Defendant, Ductant, and other co-conspirators used at 2700 S. University Drive, #203, Miramar (hereinafter, the "Miramar Office"). Such tangible evidence includes, among other things: USAA Bank victims' bank statements; USAA Bank victims' credit cards; counterfeit driver's licenses in USAA Bank victims' names; USAA Bank victims' checks; handwritten ledgers with victim information; USAA Bank victims' passwords, addresses, and bank account information. By way of example:

a) In the Miramar Office, investigators found, among other things: post-it notes with 64 victims' names, along with email addresses, bank information, driver's license numbers, phone numbers, routing numbers, logins, and passwords belonging to

USAA victims (among others). The mailing addresses on the post-it notes are the addresses to which the fraudulent loan checks and credit cards obtained in this scheme were mailed (not the true addresses for the victims). The post-it notes contain the common password information for these victims' online accounts created in furtherance of the scheme. Investigators also found the actual credit cards fraudulently obtained in the names of USAA victims, and others believed to be victims of fraud.

b) In Defendant's Pembroke Pines residence, investigators found, among other things: copies of Citibank mail to USAA victims S.W. and J.S., along with a copy of a Wells Fargo check with Sixta's forged signature made out to "Well-Connected" (a company for which Defendant is the registered agent); identity theft victims' USAA credit card statements, TD Bank check books, credit and debit cards, and bank account statements; a written ledger with 23 victims' names and the status of these credit cards as accepted or rejected; counterfeit Florida driver licenses; and thirty-eight (38) $500 non-negotiated Western Union Money orders purchased with fraudulently obtained USAA debit cards.

14. With respect to digital evidence, the government will offer evidence from numerous cell phones and computers attributable Defendant and his co-conspirators, which were found during the execution of the search warrants at the Pembroke Pines Residence and the Miramar Office. The digital evidence included the following: text messages, photographs, emails, chats, screen shots, and voicemails, such as pictures of victim checks, victim credit cards, victim counterfeit driver's licenses, login passwords for victims, and victim email accounts. By way of example:

a) Emails and email account settings on Defendant's cell phone establish that Defendant controlled hundreds of victim email accounts, including 14 victim email accounts used in connection with the procurement of USAA loans and the creation of unauthorized bank accounts. The mailboxes of these victim email accounts were stored on Defendant's cell phone, meaning that Defendant could (and did) send and receive email messages from the victim account using the mail application on his phone.

b) Emails found on a computer located in the Miramar Office contained dozens of victims' PII and other sensitive security information regarding, home/business addresses, Medical Doctor Licenses, passwords/access numbers, driver's license numbers, USAA member numbers, height, social security numbers, city where mother was born, name of first girlfriend, and Credit Karma passwords.

c) Text message content (including attachments) establish that Defendant and his co-conspirators exchanged images of victim credit cards (including USAA victim S.W.), victim driver's licenses (including USAA victim J.H.), "informed delivery" updates (i.e., USPS tracking) of victim card services, and bank loan information, among other things.

d) Text message content (including attachments) establishes that Defendant and his co-conspirators exchanged images and tracking numbers and pick-up addresses of victim mail/packages that they were tracking (e.g., a FedEx label for a package to victim S.W., the victim whose USAA credit cards statements and TD check books, among other things, were found in Defendant's Pembroke Pines Residence).

e) Pictures of victim credit cards, USAA applications, victim passwords, PIN numbers, bank accounts, and other information stored on Defendant's cell phone were Geo tagged at the location of the Miramar Office and the Pembroke Pines Residence.[2]

15. Additionally, IP records obtained by subpoena further establish the link between Defendant, his co-conspirators, and the criminal activity. For example:

a) The Comcast IP address "73.245.208.9" is registered to Defendant and has the service address of the Pembroke Pines Residence. This IP address was used multiple times to access victim bank accounts.

b) The Comcast IP address "66.229.33.78" is registered to Venturion, LLC and has the service address of the Miramar Office (which is the registered business address for Venturion, LLC) and the location where law enforcement observed Defendant and Ductant spending significant time. This IP address was used multiple times to access victim accounts.

[2] Geo-tagging is the process of attaching location information in the form of geographical metadata to digital media like web sites, videos, and photographs. The information included in a geo-tag may include place co-ordinates (latitude and longitude), bearings, altitude, distances, or even place names.

16. Records and testimony from USAA Bank witnesses will establish that the conspiracy carried out by Defendant and his co-conspirators caused USAA Bank to suffer a loss of $1,045,325.

IV. Fraudulent EIDL and PPP Loans (CARES Act Fraud)

17. The government will offer tangible, digital, and documentary evidence establishing that Defendant and his co-conspirators fraudulently obtained COVID-19 pandemic relief funds from the SBA, both through the EIDL program and the PPP, by using stolen identities and making other material misrepresentations.

18. For example, the government will show that Defendant and his co-conspirators submitted and caused the submission of fraudulent EIDL and PPP applications to the SBA from the IP address at the Miramar Office, among other places. Three of these applications were submitted using stolen identities of three non-incarcerated victims, "W.S.", "K.R.", and "M.S." Defendant and his co-conspirators also used stolen identities to open bank accounts to receive such EIDL proceeds. Two of such bank account were opened at USAA Bank in the name of M.W., an inmate with the Florida Department of Corrections with a scheduled release date in 2037. Defendant's cell phone contained the email account for M.W., the images of a counterfeit driver's licenses for M.W. and W.S., and the images of the debit cards linked to the fraudulent M.W. bank accounts at USAA Bank. The physical counterfeit license for victim inmate M.W. and the physical debit cards were found in Defendant's Pembroke Pines Residence. Those debit cards were used to withdraw the EIDL proceeds through the purchases of thousands of dollars in Western Union Money Orders at Publix supermarkets, which Defendant and his co-conspirators endorsed and deposited into their respective accounts (discussed in greater below).

19. Identity theft victims Rivest and Steiner reported the fraudulent loans to their local police departments (Cape Coral and Broward Sheriff's Office). They provided sworn affidavits and are prepared to testify that they did not apply for these loans or open the bank accounts used to receive the loan proceeds.

20. Defendant and his co-conspirators also used stolen PII of inmates in federal prison, such as S.W., S.P., and J.E., to fraudulently acquire PPP loans. At the direction of Defendant and his co-conspirators, the proceeds of these fraudulent PPP loans were electronically deposited into fraudulently created T-Mobile bank accounts in the inmates' names, which Defendant and his co-conspirators withdrew using debit cards linked to such fraudulent accounts. For example, the debit cards for the PPP loan to S.W. was found in Defendant's Pembroke Pines Residence; the debit cards for the PPP loan to J.E. and S.P. were found in the Miramar Office. As discussed below, bank records show that Defendant and his co-conspirators diverted the proceeds of these PPP loans for their own use and benefit, including Defendant paying rent for the Pembroke Pines Residence.

21. Records and testimony from the SBA witnesses will establish that, in total, Defendant and his co-conspirators were responsible for at least 16 fraudulent SBA loans totaling $2,052,500.

V. Deposit and Withdrawal of Fraud Proceeds

22. The government will offer bank records obtained by subpoena, including ATM surveillance photos, to establish that Defendant (and Ductant) deposited several fraudulently obtained USAA loan proceed checks into fraudulently created victim bank accounts that they controlled, and then withdrew the proceeds from those victim bank accounts through forged checks (among other withdrawal methods). The following are examples related directly to Defendant:

a) On January 20, 2020, Defendant deposited fraudulently obtained USAA Bank loan check number 0008975776 in the amount of $50,000 payable to an Identity Theft Victim having initials "C.S.," a federal inmate who had been in custody since September 2014. Bank records establish that this deposit went into a Wells Fargo checking account ending 6745 that was fraudulently opened online on January 4, 2020 in the name of C.S. using a counterfeit driver's license number. Wells Fargo ATM photos clearly show Defendant depositing the $50,000 check on January 20, 2020 at approximately 8:03 p.m. ATM photos also show Defendant later withdrawing the proceeds of the fraudulent USAA bank loan check by depositing into his business bank account for Well-Connected Marketing forged checks drawn from C.S.'s fraudulent account for phony services. For example, on February 4, 2020, at approximately 7:54 p.m., Defendant deposited into Wells Fargo account 5615 forged check #102 payable to "Well-Connected Marketing" in the amount of $18,000 for "Home System," which was drawn from C.S.'s fraudulent account. An image of the counterfeit Florida driver's license for C.S. used in the scheme was found in Defendant's cell phone.

b) On February 19, 2020, Defendant deposited USAA Bank loan check number 0008988796 in the amount of $49,825 payable to Identity Theft Victim having initials J.S., an inmate with the California Department of Corrections who had been in custody since May 24, 2016. Bank records establish that this deposit went into a Wells Fargo checking account ending 4184 that was fraudulently opened online on February 11, 2020 in the name of J.S. using a counterfeit driver's license number. ATM photos clearly show Defendant depositing the $49,825 check on

February 19, 2020 at approximately 9:58 p.m. An image of the counterfeit Florida driver's license for J.S. used in the scheme was found in Defendant's cell phone.

c) On March 2, 2020, Defendant deposited USAA Bank loan check number 0009529439 in the amount of $39,500 payable to Identity Theft Victim J.H., a federal inmate who had been in custody since December 10, 2018. Bank records establish that this deposit went into a Wells Fargo checking account ending 4184 that was fraudulently opened online on January 29, 2020 in the name of J.H. using a counterfeit using a counterfeit driver's license number. ATM photos clearly show Defendant depositing the $39,500 check on March 2, 2020 at approximately 8:18 p.m. ATM photos also show Defendant later depositing into his business bank accounts (Well-Connected and Pompano 318) forged checks drawn from J.H.'s fraudulent account for phony services. For example, on March 11, 2020, Defendant, at approximately 7:13 p.m., Defendant deposited into Wells Fargo account ending 5615 forged check #101 payable to "Well-Connected Marketing" in the amount of $9,000 for "Home System," which was drawn from J.H.'s fraudulent account. On March 20, 2020, at approximately 11:20 p.m., Defendant deposited into Wells Fargo account ending 1026 forged check #105 payable to "Pompano 318 LLC" in the amount of $8,800 for "Roof repair," which was drawn from J.H.'s fraudulent account. A picture of the counterfeit Florida driver's license for J.H. used in the scheme was found in cell phone communications/pictures shared between Defendant and Ductant.

23. Bank records and other records also establish that Defendant and his co-conspirators diverted fraud proceeds to themselves by using fraudulently obtained credit and debit

cards issued to identity theft victims to purchase Western Union Money Orders (WUMOs) at Publix and Winn Dixie supermarkets, which Defendant and his co-conspirators deposited into their personal and business bank accounts. For example, the two USAA Visa debit cards in the name of inmate victim M.W. and one T-Mobile Master Card in the name of victim S.W.—which cards were physically found in Defendant's Pembroke Pines Residence—were used to purchase the following thirty-three (33) WUMOs, each $500 payable to Defendant's company Well-Connected Marketing Group LLC, which Defendant endorsed and deposited into his bank account at PNC Bank ending in #0188.

24. Additionally, bank records show that Defendant diverted fraud proceeds by swiping fraudulently obtained victim credit and debit cards for payments to his purported businesses. For example, Defendant caused his company Well Connected Marketing to charge a USAA Bank American Express card ending 3898, issued in Identity Theft Victim J.S.'s name, the following: $3,160.05 on October 26, 2019, $2,685.35 on October 31, 2019, and $4,225.60 on November 21, 2019. The government will offer evidence of credit card swipers and other point of sale devices found inside the Miramar Office and the Pembroke Pines Residence.

25. As a result of Defendant's participation in the conspiracy, Defendant and his co-conspirators are responsible for causing an actual loss of $3,097,825, of which $1,045,325 in loss was incurred by USAA Bank and $2,052,500 in loss was incurred by the SBA. Defendant and his co-conspirators used the fraudulently obtained proceeds to enrich themselves and others through approximately May 2021.

CONCLUSION

26. The facts and supporting evidence set forth in this proffer, which do not include all the facts or all the evidence that the United States would use at trial, are sufficient to prove beyond a reasonable doubt the elements of conspiracy to commit bank fraud and wire fraud, in violation of Title 18, United States Code, Section 1349, and aggravated identity theft, in violation of Title 18, United States Code, Section 1028A(a)(1), and that Defendant Kervens Saint-Hilaire is in fact guilty of those offenses as charged in Count 1 and Count 16, respectively, of the Indictment.

MARKENZY LAPOINTE
UNITED STATES ATTORNEY

Date: 01/29/2024 By: _____
DAVID A. SNIDER
ASSISTANT UNITED STATES ATTORNEY

Date: 01/29/2024 _____
SHELDON ZIPKIN
ATTORNEY FOR DEFENDANT

Date: 01/29/2024 _____
KERVENS SAINT-HILAIRE
DEFENDANT