IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF FLORIDA TALLAHASSEE DIVISION

UNITED STATES OF AMERICA

v. **CASE NO. 4:21cr36-AW-MAF-2**

NICOLAS CARL RAMIREZ

_____/

STATEMENT OF FACTS

The parties agree with the truthfulness of the following factual basis for the defendant's guilty plea. The undersigned parties further agree that not all of the facts known from this investigation are contained in this brief summary. Defendant admits that, if this case were to proceed to trial, the Government could prove the following facts beyond a reasonable doubt:

On March 27, 2020, Congress passed the $2.2 trillion Coronavirus Aid, Relief, and Economic Security ("CARES") Act, which in part provided economic relief for taxpayers nationwide in response to the COVID-19 pandemic. The aid package included an Economic Impact Payment [("EIP"), also known as a "Coronavirus Stimulus check" or "Coronavirus Stimulus payment"] of $1,200 to individuals, so long as their last annual adjusted gross income was less than $75,000. Payments were distributed by the United States Treasury via direct

deposit, or by mail using the latest address on file with the Internal Revenue Service ("IRS").

On May 2, 2020, Tallahassee Police Department ("TPD") received a report from A.H., who advised TPD that her $1,200 EIP had been mailed to an old residential address that she used for her W-2 (2700 West Pensacola Street, Apartment 1223, Tallahassee, FL 32304). Records from the United States Treasury indicated that A.H.'s EIP treasury check was placed in mail with the United States Postal Service on or about May 24, 2020. A.H. also advised that she received a call from TD Bank (in South Carolina) informing her that an account using her name, social security number, and her old West Pensacola Street address had been created online. A.H. stated she only banked with Bank of America and had no knowledge of the TD Bank account that was created. Further, A.H. advised that she was told by TD Bank that her EIP check had been deposited into the TD Bank account and that phone number (850) 462-2335 was used when the account was opened in her name. The endorsement on the rear on A.H.'s EIP treasury check purported to be that of A.H.; however, A.H. told investigators that the signature was false and not hers.

TD Bank records show that the account opened in the name of A.H., using A.H.'s Social Security number and date of birth, was opened electronically on May 1, 2020, and A.H.'s Treasury check was deposited into that account via mobile

deposit on the same day. TD Bank records further show that the phone numbers (850) 462-2335 and (786) 709-3353 (which was later discovered to be Co-Defendant Joe Catala's T-Mobile phone number) were registered to the account; those phone numbers were later linked to Co-Defendant Catala. The TD Bank records also show that two Zelle transfers were made to (Co-Defendant) "Clonet Charmant" on May 4, 2020, from that account. Law enforcement agents later interviewed Co-Defendant Charmant and he confirmed that the two Zelle transfers were sent to him by Co-Defendant Catala.

During the course of the investigation, agents learned that phone number (850) 462-2335 was one of the phone numbers belonging to TextNow, Inc. for use by its customers. TextNow, Inc. records revealed that on November 21, 2019, at approximately 8:05 AM UTC, user account "drewhunchie" was created utilizing email address drewhunchie@gmail.com, and that on April 22, 2020, at approximately 3:00 AM UTC, "drewhunchie" took ownership of phone number (850) 462-2335. TextNow, Inc. also provided IP logs for recent activity associated with the username "drewhunchie" for April 2020 and May 2020 that reflected the same two IP addresses being used – 184.102.14.253 and 71.209.94.161.

TextNow, Inc. also provided call and message logs for phone number (850) 462-2335 which revealed at least one call to Kiku Japanese Fusion in Tallahassee,

FL. TextNow, Inc. also provided call logs that reflected phone number (850) 462-2335 also made calls to TD Bank.

On May 13, 2020, agents went to Kiku Japanese Fusion in Tallahassee. An employee there provided a copy of an order invoice dated April 30, 2020, for a customer whose initials were "A.C." with a phone number of (850) 462-2335. The order was paid for using a debit/credit card ending in 1419 (belonging to Co-Defendant Catala) with a billing ZIP code of 34953 (associated with the Port St. Lucie, FL area).

CenturyLink records indicated that IP addresses 184.102.14.253 and 71.209.94.161 were assigned to a subscriber whose billing name is "Villa Del Lago" with a service address of 2700 West Pensacola Street, Unit 1223, Tallahassee, FL (which is now known as "The Social 2700 Student Spaces" apartment complex) since July, 26, 2010. The Social 2700 used to be known as "Villa Del Lago."

Defendant Ramirez, Co-Defendant Charmant, and Co-Defendant Catala were all friends and graduates of (St. Lucie West) Centennial High School in Port St. Lucie, FL, and Co-Defendant Catala was a frequent guest of Defendant Ramirez' at 2700 West Pensacola Street, Apartment 1223, Tallahassee, FL 32304. Each resident of Apartment 1223 had a mailbox key for the locked mailbox assigned to that apartment unit, but Ramirez and a former roommate, A.I., lost

theirs. Before another roommate moved out of Apartment 1223 in March 2020, he gave his mailbox key to Co-Defendant Catala. Defendant Ramirez and Co-Defendant Catala were involved in a credit card scam since August 2019, and Co-Defendant Catala, using his laptop, searched the "Dark Web" to obtain unknown persons' personally identifiable information ("PII") at the apartment in Tallahassee as part of the credit card scam.

Further investigation revealed a scheme to defraud multiple U.S. bank customers using Zelle, fraudulent account applications, and through fraudulent use of debit card numbers to make purchases. These customers banked with Austin Telco Credit Union, Bank of America, Bank of Hawaii, BB&T, Discover Bank, Frist Republic Bank, GBC International Bank, Innovations Federal Credit Union (headquartered in Panama City, FL), JPMorgan Chase, TD Bank, and UMB Bank – all were federally insured at all times relevant to this investigation. The defendants used Zelle to transfer funds from victim accounts (with financial institutions located nationwide) into the accounts of the defendants.

Records obtained from Zelle (Early Warning Services) reflect that Co-Defendant Catala and Defendant Ramirez fraudulently received funds from a customer account at Innovations Federal Credit Union (headquartered in Panama City, Florida) into their bank accounts using Zelle. Specifically, Defendant Ramirez fraudulently and knowingly received a transfer of $200 into his Chase

account from the account belonging to S.P. (who Defendant Ramirez knew to be a real person), and Co-Defendant Catala fraudulently and knowingly received two transfers of $150 each into his BB&T account from the account belonging to S.P. These transfers were done without authority from S.P., and the defendants used S.P.'s name and bank account to make the transfers, again without S.P.'s permission.

ELEMENTS OF THE OFFENSE

i. Conspiracy to Commit Bank Fraud and Wire Fraud – 18 U.S.C. § 1349

Elements to be proven beyond a reasonable doubt:

1) two or more persons, in some way or manner, agreed to try to accomplish a common and unlawful plan to commit bank fraud and wire fraud, as charged in the indictment; and

2) the Defendant knew the unlawful purpose of the plan and willfully joined in it;

Adapted from 11th Circuit Pattern Jury Instructions § O54.

ii. Bank Fraud - 18 U.S.C. § 1344

Elements to be proven beyond a reasonable doubt:

1) the Defendant knowingly carried out or attempted to carry out a scheme to defraud a financial institution or to get money, assets, or other property from a financial institution by using false or fraudulent pretenses, representations, or promises about a material fact;

2) the false or fraudulent pretenses, representations, or promises were material;

3) the Defendant intended to defraud the financial institution or someone; and

4) the financial institution was federally insured.

11th Circuit Pattern Jury Instructions § O52.

iii. Aggravated Identity Theft – 18 U.S.C. § 1028A

Elements to be proven beyond a reasonable doubt:

(1) The Defendant knowingly transferred, possessed, or used another person's means of identification;

(2) The Defendant did so without lawful authority[1];

(3) The Defendant knew the means of identification belonged to an actual person[2], and

(4) The Defendant did so in relation to bank fraud.

11th Circuit Pattern Jury Instructions § O40.3.

[1] In United States v. Zitron, 810 F.3d 1253, 1260 (11th Cir. 2016) (per curiam), the Eleventh Circuit found that the defendant used the victim's identity "without lawful authority" in two ways: (1) the defendant did not have permission to use the victim's identity, and (2) the defendant used the victim's means of identification for an unlawful purpose. See also United States v. Joseph, 567 F. App'x 844, 848 (11th Cir. 2014) (per curiam) (unpublished).

[2] Does not appear in the 11th Circuit Pattern Jury Instructions.

William J. Cone, Jr.
Attorney for Defendant

11/23/21
Date

Nicolas Carl Ramirez
Defendant

11/23/2021
Date

JASON R. COODY
Acting United States Attorney

Justin M. Keen
Florida Bar No. 021034
Assistant United States Attorney
Northern District of Florida
111 North Adams Street, 4th Floor
Tallahassee, FL 32301
850-942-8430
Justin.Keen@usdoj.gov

11/30/2021
Date