UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK
- - - - - - - - - - - - - - - - - X

UNITED STATES OF AMERICA :

- v. - : **SUPERSEDING INFORMATION**

ROMANA LEYVA, : S3 19 Cr. 667 (PAC)

Defendant. :

- - - - - - - - - - - - - - - - - X

COUNT ONE
(Conspiracy to Commit Wire Fraud)

The United States Attorney charges:

OVERVIEW OF THE SCHEME

1. From at least in or around February 2015 up to and including in or around December 2018, ROMANA LEYVA, the defendant, and others known and unknown, were members of a criminal fraud ring (the "Fraud Ring") based in the United States and India that committed a technical support fraud scheme targeting elderly victims located across the United States and Canada, including in the Southern District of New York. The primary objective of the Fraud Ring's technical support fraud scheme was to trick and deceive victims into believing that their computers were infected with malware, and then convince them to pay hundreds or thousands of dollars to the Fraud Ring for phony computer repair services. Over the course of the

conspiracy, the Fraud Ring generated more than $10 million in proceeds from at least approximately 7,500 victims.

MEANS AND METHODS OF THE CONSPIRACY

2. The scheme generally worked as follows. First, the Fraud Ring caused pop-up windows to appear on victims' computers. The pop-up windows claimed, falsely, that a virus had infected the victim's computer. The pop-up window directed the victim to call a particular telephone number to obtain technical support. In at least some instances, the pop-up window threatened victims that, if they restarted or shut down their computer, it could "cause serious damage to the system," including "complete data loss." In an attempt to give the false appearance of legitimacy, in some instances the pop-up window included, without authorization, the corporate logo of a well-known, legitimate technology company. In fact, no virus had infected victims' computers, no harm would have resulted from shutting down or restarting the computer, and the technical support numbers were not associated with the legitimate technology company. Rather, these representations were false and were designed to trick victims into paying the Fraud Ring to "fix" a problem that did not exist. And while the purported "virus" was a hoax, the pop-up window itself did cause various victims' computers to completely "freeze," thereby preventing these victims from accessing the files in their computer --

which also caused some victims to call the phone number listed in the pop-up window.

3. Indeed, a victim who called the purported technical support phone number reached a call center associated with the Fraud Ring. Conspirators at the call center requested permission to obtain remote access to victim computers. Once granted access, the member of the Fraud Ring connected remotely to the victim's computer, made diagnostic tools appear on the victim's computer screen, and falsely repeated that the computer was infected with a virus, and informed the victim that he or she could fix the purported problem in exchange for a fee. The fee varied depending on the purported "service" selected (*e.g.*, one-time, one year, lifetime support, etc.) and typically ranged between several hundred dollars, and several thousand dollars. If a victim agreed verbally to one of these arrangements, the member of the Fraud Ring would download and run a freely available anti-virus tool, and then leave a text file on the desktop of the victim's computer with specific payment instructions.

4. In some cases, certain victims were re-victimized in connection with a purported "refund" of their original payment to the Fraud Ring. For example, a victim was initially defrauded out of several hundred dollars due to the technical support fraud explained above; that victim had paid the Fraud

Ring to remove the purported virus from their computer and to receive "lifetime" technical support. Later, the Fraud Ring contacted that victim to say that the technical support company that had promised lifetime support was going out of business and wanted to refund the victim, as the company could no longer provide lifetime support. Through the "refund" process, the Fraud Ring gained access to the victim's bank account; claimed to have paid out too large of a refund, due to a typographical error (*e.g.*, a refund of $4,500 instead of the intended refund amount of $450); and instructed the victim to "reimburse" the Fraud Ring thousands of dollars, through gift cards.

5. Over the course of the conspiracy, the Fraud Ring generated more than $10 million in proceeds from victims through various means of payment, including but not limited to credit cards, personal checks, postal money orders, and gift cards. Over the course of the conspiracy, the Fraud Ring generally transitioned from receiving payments via credit card and personal check -- both of which could be reversed, for a time, after a victim's payment -- to receiving payments via postal money orders and gift cards, which could not later be reversed or clawed back.

6. At all times relevant to this Information, ROMANA LEYVA, the defendant, was a Nevada-based member of the Fraud Ring. Among other things, LEYVA created several fraudulent

corporate entities that were used to receive fraud proceeds from victims, recruited others (including through misrepresentations) to register fraudulent corporate entities that became part of and facilitated the activities of the Fraud Ring, and assisted others in setting up fraudulent corporate entities and bank accounts, including coaching them to make misrepresentations to bank employees where necessary.

STATUTORY ALLEGATIONS

7. From at least in or around February 2015 up to and including in or around December 2018, in the Southern District of New York and elsewhere, ROMANA LEYVA, the defendant, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, wire fraud, in violation of Title 18, United States Code, Section 1343.

8. It was a part and object of the conspiracy that ROMANA LEYVA, the defendant, and others known and unknown, did willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of

executing such scheme and artifice, and aided and abetted the same, to wit, LEYVA engaged in a technical support fraud scheme to deceive victims that their computers were infected with malware, to induce them to pay for computer repair services that they did not need and make other unnecessary payments, and sent and received, and caused others to send and receive, interstate and foreign text messages and phone calls, to and from the Southern District of New York and elsewhere, in furtherance of that scheme, in violation of Title 18, United States Code, Section 1343.

Overt Acts

9. In furtherance of the conspiracy, and to effect the illegal object thereof, ROMANA LEYVA, the defendant, together with others known and unknown, committed the following overt acts, in the Southern District of New York and elsewhere:

a. On or about February 25, 2015, LEYVA registered a fraudulent corporate entity used by the Fraud Ring to defraud victims.

b. On or about April 26, 2015, LEYVA opened a bank account for that fraudulent corporate entity, which was used to receive fraud proceeds from victims.

c. On or about April 1, 6, and 7, 2016, LEYVA sent a WhatsApp message to a co-conspirator not named as a defendant herein ("CC-1"), who was in New York, in which LEYVA

coached CC-1 through the process of registering an LLC through which the Fraud Ring received fraud proceeds from victims, and in which LEYVA supplied the name for that LLC.

d. On or about April 24, 2016, LEYVA sent a WhatsApp message to CC-1, in which LEYVA coached CC-1 -- who was opening bank accounts that were used to receive fraud proceeds from victims -- to lie to the bank employee about how long CC-1 had worked in online IT support.

e. On or about February 8, 2018, the Fraud Ring (i) caused a pop-up window to appear on a particular victim's computer, which was located in the Southern District of New York, which prevented that victim from accessing his data, files, and information and thus impaired the availability of his data, and (ii) directed that victim to pay CC-1's LLC a fee in order to regain access to his data.

(Title 18, United States Code, Section 371.)

COUNT TWO
(Conspiracy to Intentionally Damage a Protected Computer)

The United States Attorney further charges:

10. The allegations contained in paragraphs 1 through 6 of this Information are repeated and realleged as if fully set forth herein.

11. From at least in or around February 2015 up to and including in or around December 2018, in the Southern District

of New York and elsewhere, ROMANA LEYVA, the defendant, and others known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit an offense against the United States, to wit, intentional damage of a protected computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), and (c)(4)(B)(i).

12. It was a part and object of the conspiracy that ROMANA LEYVA, the defendant, and others known and unknown, would and did knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage without authorization to a protected computer, and caused loss to one and more persons during a one-year period affecting protected computers aggregating at least $5,000 in value, to wit, LEYVA and her co-conspirators caused pop-up windows to appear on victims' computers, which -- in several instances -- caused victims' computers to completely freeze, thereby preventing victims' access to their data, files, and information and thus impairing the availability of their data, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(c)(4)(A)(i)(I), and (c)(4)(B)(i).

Overt Act

13. In furtherance of the conspiracy, and to effect the illegal object thereof, ROMANA LEYVA, the defendant, together

with others known and unknown, committed the following overt act, in the Southern District of New York and elsewhere:

a. On or about February 8, 2018, the Fraud Ring (i) caused a pop-up window to appear on a particular victim's computer, which was located in the Southern District of New York, which prevented that victim from accessing his data, files, and information and thus impaired the availability of his data, and (ii) directed that victim to pay CC-1's LLC a fee in order to regain access to his data.

(Title 18, United States Code, Section 371.)

FORFEITURE ALLEGATIONS

14. As a result of committing the offense alleged in Count One of this Information, ROMANA LEYVA, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any and all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of said offense, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense.

15. As a result of committing the offense alleged in Count Two of this Information, ROMANA LEYVA, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 1030(i), any and all property, real or

personal, constituting or derived from, any proceeds obtained directly or indirectly, as a result of said offense, and any and all personal property that was used or intended to be used to commit or to facilitate the commission of said offense, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense.

Substitute Assets Provision

16. If any of the above-described forfeitable property, as a result of any act or omission of the defendant:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with, a third person;

c. has been placed beyond the jurisdiction of the Court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), and Title 28, United States Code, Section 2461, to seek forfeiture of any other property of

the defendant up to the value of the forfeitable property described above.

(Title 18, United States Code, Sections 981, 1030; Title 21, United States Code, Section 853; and Title 28, United States Code, Section 2461.)

/s/
AUDREY STRAUSS
United States Attorney

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

ROMANA LEYVA,

Defendant.

SUPERSEDING INFORMATION

S3 19 Cr. 667 (PAC)

(18 U.S.C. § 371.)

AUDREY STRAUSS
United States Attorney