UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

CASE NO. 21-cr-20380-RNS

UNITED STATES OF AMERICA,

v.

KENNY TERLENT,
a/k/a "KenLa,"
a/k/a "headhuncho7700,"

Defendant.
_____/

FACTUAL PROFFER

Defendant, Kenny Terlent, a/k/a "KenLa," a/k/a "headhuncho7700" (the "Defendant"), his counsel, and the United States of America agree that, had this case proceeded to trial, the United States would have proven the following facts beyond a reasonable doubt:

In the summer of 2020, law enforcement obtained search warrants for the phones and social media accounts of a co-conspirator (CC1) of the Defendant. Those phones and social media accounts showed that CC1 was involved in access device fraud and aggravated identity theft with the Defendant, including through the Defendant's use of his own cell phones and iCloud account (kennyterlent400@icloud.com). On September 23, 2020, law enforcement obtained a search warrant for that iCloud account, which the Defendant later admitted was his. A review of the account showed that the Defendant was in possession of thousands of unauthorized access devices, and that he possessed those access devices with the intent to defraud.

For instance, during a review of the material obtained from the Defendant's iCloud account, law enforcement found that the Defendant had used a Chime Account in the name of victim J.G. (the "J.G. Chime Account"). Chime is a mobile application that allows people to send and receive money – among other things. Records received from Chime showed that the J.G.

Chime Account was opened in J.G.'s name using his personally identifiable information. However, the address and phone number on the account were not those of J.G., but instead were an address and phone number provided by the Defendant. Based on a review of data obtained from Chime, the Defendant used the J.G. Chime Account to receive payments from unemployment fraud and COVID fraud. The Defendant also had numerous conversations related to the use of the unauthorized access devices in his possession.

During the review of the iCloud account, law enforcement found unauthorized access devices belonging to significantly more than fifteen victims, including names, dates of birth, and social security numbers belonging to individuals other than the defendant. These access devices included the name, address, date of birth, and social security number (ending in 4996) belonging to victim L.S. Victim L.S. was interviewed by law enforcement and stated that she does not know the Defendant, and she did not authorize the Defendant to possess or use her personally identifiable information. Law enforcement also located the name, date of birth, social security number (ending in 8487) and other information belonging to victim K.S. Victim K.S. was interviewed by law enforcement and stated that she does not know the Defendant and she did not authorize the Defendant to possess or use her personally identifiable information.

In addition to the above victims, the Defendant had a PDF stored in his iCloud titled "I'm Rich Bitch 🖕." The PDF is a 7,620 page document containing the personally identifiable information from thousands of victims, including their names, dates of birth, addresses, social security numbers, and other information. On page 1 of the PDF, the top of the document lists the name of a medical facility in Orlando. In that PDF, law enforcement found the personal information of victims J.A. (SSN # 7157) and D.A. (SSN # 3236), including their names, dates of birth, social security numbers, and other information. Both victims were interviewed by law

enforcement, and confirmed that they did not know the Defendant, and did not authorize him to possess their personal information.

On June 24, 2021, law enforcement executed a search warrant at the Defendant's residence. That search warrant allowed for the seizure and search of any cell phones located within the residence, or on the Defendant's person. During the execution of the warrant, law enforcement approached the Defendant outside of his residence. The Defendant ran from law enforcement, slipped, fell, and then threw his cell phone into the lake in his backyard.

Law enforcement retrieved the Defendant's cell phone from the lake, and searched it pursuant to the search warrant. Within the phone, law enforcement located the access devices of at least 15 or more victims. This included the names, dates of birth, social security numbers, and other information belonging to individuals other than the Defendant. Within that phone, law enforcement located the following unauthorized access devices, among many others: (1) the social security number (ending in 7330), DOB, and addresses of victim B.W.; (2) the social security number (ending in 8261), DOB and addresses of victim K.S. (different K.S. than earlier); and (3) the social security number (ending in 6572), DOB, and address of victim M.F. This PII came from various "carding" or "SSN" websites, such as "unicc.cm," and "robocheck.cc." The Defendant was not authorized by the victims to possess that PII. Further, the phone contained a multitude of evidence that these unauthorized access devices were used to submit fraudulent unemployment claims.

Also in the Defendant's residence, law enforcement located the Defendant's Glock 19, bearing serial number BBWB707. That Glock 19 had an "auto sear" affixed to it, which is colloquially called a "switch." An auto sear is a device that allows semi-automatic firearms to fire in fully automatic mode. The firearm was found wrapped up in a blanket, and hidden in a clothes hamper. Within the same blanket were a laptop, and another one of the Defendant's phones. The

phone had a Chime card in J.G.'s name within the phone case (the same J.G. mentioned above). Also, this phone's associated iCloud account was kennyterlent400@icloud.com. Law enforcement test-fired the Glock 19, and confirmed that it was capable of firing in fully automatic mode, thus qualifying as a machine gun. The Defendant does not have a permit to possess a machine gun.

Based on a review of the Defendant's iCloud account, law enforcement determined that, on March 27, 2021, the Defendant sent a text message to a group of associates that included a picture of what appears to be the same Glock (with a "switch" installed) that was recovered from the Defendant's residence. After sending that picture, the Defendant texted "Switch on that Glock that bitch keeps switching." Also, while reviewing the cell phone that TERLENT threw into the lake, law enforcement located a photograph of what appears to be the same Glock (with "switch" installed).

Also in the Defendant's residence, in the Defendant's dresser, law enforcement located mail in other people's names, bank documents in other people's names, 3-4 small cell phones, one round of 40 caliber ammunition, and an additional Chime card in a victim's name.

On June 24, 2021, the Defendant gave a post-*Miranda* statement to law enforcement. With regard to the iCloud account, the Defendant confirmed that that was his account, and that the phone number associated with the account was his as well.

In all, the Defendant possessed 2,760 unauthorized access devices with the intent to defraud. His possession of those access devices affected interstate commerce in that: (1) a large number of the victims were located out of state; (2) the internet (moving in interstate commerce) was used to procure a number of the unauthorized access devices; (3) the banks that were the subject of the fraud are located in other states and operate in interstate commerce; and (4) the Defendant communicated via cellular networks and social media to further his fraud.

request of all necessary and appropriate documentation to deliver good and marketable title, consenting to all orders of forfeiture, and not contesting or impeding in any way with any criminal, civil or administrative forfeiture proceedings.

12. This is the entire agreement and understanding between this Office and the Defendant. There are no other agreements, promises, representations, or understandings.

JUAN ANTONIO GONZALEZ
ACTING UNITED STATES ATTORNEY

Date: 10/21/21 By: _____
FREDERIC C. SHADLEY
ASSISTANT UNITED STATES ATTORNEY

Date: 10/21/21 By: _____
ANDREW RIER, ESQ.
ATTORNEY FOR DEFENDANT

Date: 10/21/21 By: Kenny Terlent
KENNY TERLENT
DEFENDANT