HEE 9.4.2020

ZAM&CMR: 2019R00813

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

UNITED STATES OF AMERICA	*	
	*	**CRIMINAL NO.** JKB-20-195
v.	*	
	*	**(Wire Fraud, 18 U.S.C. § 1343; Unauthorized Access of a Protected Computer in Furtherance of Fraud, 18 U.S.C. §§ 1030(a)(4) & (b); Intentional Damage to a Protected Computer, 18 U.S.C. § 1030(a)(5)(A); Aggravated Identity Theft, 18 U.S.C. § 1028A; Wire Fraud Conspiracy, 18 U.S.C. § 1349; Forfeiture, 18 U.S.C. § 981)**
JORDAN K. MILLESON and KYELL A. BRYAN,	*	
Defendants.	*	

****

SUPERSEDING INDICTMENT

COUNTS ONE THROUGH SIX
(Wire Fraud)

The Grand Jury for the District of Maryland charges that:

At all times material to this Superseding Indictment:

The Defendants

1. Defendant **JORDAN K. MILLESON ("MILLESON")**, born in July 1999, was a resident of Lutherville, Baltimore County, Maryland. **MILLESON** was a computer "hacker", who accessed various computers, computer networks, and electronic accounts without authorization, which allowed him to carry out and further various criminal offenses and schemes.

2. Defendant **KYELL A. BRYAN ("BRYAN")**, born January 2001, was a resident of Brooklyn, New York, and later Kingston, Pennsylvania, who participated in the unauthorized takeover of wireless telephone and financial accounts which allowed him to carry out and further various criminal offenses.

Phishing

3. "Phishing" was one of the most common forms of social engineering used to induce victims into turning over sensitive data—such as personally identifiable information, passwords, and credit card details. Victims of phishing attacks were generally contacted by email, phone, or text message by persons purporting to be from reputable companies in order to induce the victims to reveal confidential data.

4. Phishing emails commonly were designed to appear as if they originated from a legitimate source, such as a well-known business, and directed the recipient to a fraudulent website link. Like the email itself, the fraudulent website had the façade of legitimacy, but the fake site was designed to induce victims to input personal information such as usernames and passwords linked to an organization's authentic website, which information was then captured by the scammer.

5. "Vishing" (Voice Phishing) was another type of phishing where impostors used internet phone services—such as Voice over Internet Protocol (VoIP)—to trick victims into turning over critical financial and personal information over the phone. Fraudsters often impersonated representatives of legitimate businesses to manipulate victims into turning over their account information or gaining unauthorized access to a company's internal computer networks.

SIM Swapping

6. In order to activate a mobile device for usage on cellular telephone networks, many devices were assigned a unique International Mobile Equipment Identity number ("IMEI") in combination with a unique subscriber identity module ("SIM"), encoded on a small removable chip or directly embedded into the device. This IMEI/SIM combination, when paired with a customer's mobile phone number assigned by a carrier, allowed a given user to authenticate on a

mobile phone carrier's network to make and receive cellular calls and text messages associated with the customer's mobile phone number.

7. Generally, "SIM Swapping" refers to a method of unauthorized takeover of a victim's wireless account by malicious actors, carried out by linking the victim's mobile phone number to a SIM installed in a device controlled by the attacker or attackers. SIM swaps were typically executed by attackers gaining unauthorized access to a wireless provider's computer networks, or with the assistance of witting or unwitting individuals who had access to the provider's networks.

8. As a result of a SIM swap, phone calls and text messages sent to the victim's mobile phone number were routed to a device controlled by the attacker or attackers, giving the attacker complete control over the victim's mobile phone number. Upon gaining control of a victim's mobile phone number, attackers often gained unauthorized access to victims' other electronic accounts—including email, social media, and cryptocurrency accounts—using various means, including intercepting "two-factor authentication" codes or resetting victims' passwords using information sent to the registered mobile phone number.

Swatting

9. "Swatting" was a criminal harassment tactic in which a person placed a false call to authorities such as a bomb threat, murder, or hostage situation to trigger a police or special weapons and tactics ("SWAT") team response to a specific address—thereby causing a life-threatening situation. Individuals engaged in swatting attacks often masked their identity and physical location by employing unattributed internet voice services—such as VoIP—to contact emergency responders and called non-emergency government telephone lines that are not recorded.

10. On or about June 26, 2019, **BRYAN**, and others known and unknown to the Grand Jury, from outside the State of Maryland, anonymously called the Baltimore County Police Department and falsely reported that he, purporting to be a resident of the **MILLESON** family residence, had shot his father at the residence. The caller threatened to shoot himself, and to shoot police officers if they attempted to confront him. This call was in fact a swatting attack, in retaliation for **MILLESON** failing to share the proceeds of the theft of digital currency, as described further in this Superseding Indictment.

The Victims

11. "Wireless Provider A" and "Wireless Provider B" were telecommunications companies, headquartered in the United States, outside of the State of Maryland, providing wireless telephone service in the United States and elsewhere. The Wireless Providers contract with third-party retail stores authorized to sell the Wireless Providers' goods and services, including wireless telephone service. Some employees of these third-party stores were given credentials that enable them to access the Wireless Providers' computer networks.

12. "Digital Currency Exchange A" was a digital currency exchange, headquartered in California. Digital Currency Exchange A allowed its customers to purchase, sell, and exchange various digital currencies, including Bitcoin, Litecoin, and Ethereum.

13. "Social Media Platform A" and "Social Media Platform B" were social media platforms owned by companies based in California which allowed users to share images, video, and text. Users of the platforms were able to send and receive direct messages and follow or be followed by other users. Some users with significant followings, often referred to as "influencers," were able to monetize their social media accounts through techniques such as sponsored links (an advertisement displayed by a search engine when someone searches for certain keywords), product

placements, and product reviews. Companies seeking to advertise their products online frequently paid social media influencers with significant followings to review and promote their products and services. Accounts with significant numbers of followers or with particularly short, unique, or memorable usernames were more highly valued because they were perceived to have a greater income potential.

14. "Individual Victim 1" was a resident of Alabama, who published content on a variety of social media platforms, including Social Media Platform A and Social Media Platform B. Individual Victim 1 had many thousands of followers on their accounts, and was able to monetize them through techniques such as sponsored links, product placements, and product reviews.

15. "Individual Victim 2" was a resident of Connecticut, and an employee of a third-party retailer for Wireless Provider A.

16. "Individual Victim 3" was a resident of Florida and owner of a digital currency investment and social media marketing company. Individual Victim 3 was the registered owner of one of his company's digital currency accounts, held at Digital Currency Exchange A.

17. "Individual Victim 4" was a resident of Rhode Island, and an investor in digital currency. Individual Victim 4 had a social media account with a two-character username, coveted by other social media users for its uniqueness and simplicity.

The Object of the Conspiracy and the Scheme and Artifice to Defraud

18. It was the object of conspiracy and the scheme and artifice to defraud to unlawfully enrich **MILLESON**, **BRYAN**, and others known and unknown to the Grand Jury, by fraudulently gaining unauthorized access to the computer networks of wireless and other electronic account

providers, and using that unauthorized access to take control of victims' electronic and financial accounts and steal amounts of digital currency.

19. Among the manner and means by which **MILLESON**, **BRYAN**, and others known and unknown to the Grand Jury, would and did carry out and execute the conspiracy and the scheme and artifice to defraud were the following:

20. **MILLESON** set up internet domains and fraudulent websites, designed to appear to be legitimate websites belonging to wireless providers, which were in fact designed to steal users' account credentials. The theft of users' account credential enabled **MILLESON**, **BRYAN**, and others known and unknown to the Grand Jury to access unsuspecting victims' electronic accounts without authorization.

21. **MILLESON** used, and caused to be used, techniques such as phishing and vishing to deceive victims into visiting the fraudulent websites and providing credentials to access their electronic accounts.

22. **MILLESON**, **BRYAN**, and others known and unknown to the Grand Jury, would use electronic account credentials stolen from employees and affiliates of the Wireless Providers to access those companies' computer networks without authorization. After obtaining unauthorized access to the computer networks of wireless providers, **MILLESON**, **BRYAN**, and others known and unknown to the Grand Jury, executed SIM swapping attacks against customers of the Wireless Providers, and took control over the customers' wireless accounts.

23. **MILLESON**, **BRYAN**, and others known and unknown to the Grand Jury, used account security features linked to these compromised mobile phone numbers to take over the mobile phone customer's online accounts, including email and digital currency accounts, facilitating their thefts of accounts and digital currency.

24. Once in control of these victim accounts, **MILLESON**, **BRYAN**, and others known and unknown to the Grand Jury, would frequently change the passwords to keep the victims from accessing their own accounts.

Overt Acts in Execution of the Conspiracy and Scheme and Artifice to Defraud

25. For the purpose of executing the aforementioned scheme and artifice to defraud, **MILLESON**, **BRYAN**, and others known and unknown to the Grand Jury, transmitted and caused to be transmitted the following internet communications in interstate commerce:

a. On or about September 23, 2017, **MILLESON**, in Maryland, sent and caused to be sent a fraudulent phishing email to Individual Victim 1, outside of Maryland, that appeared to be a legitimate email from Social Media Platform A. This email was used to steal Individual Victim 1's password, which **MILLESON** used to take over Individual Victim 1's account with Social Media Platform B.

b. On or about June 17, 2019, **MILLESON**, in Maryland, registered a fraudulent internet domain with a provider outside of Maryland. The name of the internet domain was designed to deceive others to believe it was associated with Wireless Provider A. The website hosted at Fraudulent Domain A was designed to steal the login credentials of legitimate users of Wireless Provider A's computer networks, enabling **MILLESON** to execute SIM swapping attacks against the accounts of the company's customers.

c. On or about June 25, 2019, **MILLESON**, **BRYAN**, and others known and unknown to the Grand Jury, in Maryland and elsewhere, used the credentials of Individual Victim 2 to gain unauthorized access to the computer network of Wireless Provider A, with servers outside of Maryland, and execute SIM swapping attacks, taking control of the wireless calls and text messages sent to the accounts of Individual Victim 3 and Individual Victim 4.

d. On or about June 25, 2019, **MILLESON**, **BRYAN**, and others known and unknown to the Grand Jury, in Maryland and elsewhere, took unauthorized control of Individual Victim 3's account with Digital Currency Exchange A, with servers outside of Maryland.

e. On or about June 25, 2019, **MILLESON**, in Maryland, fraudulently transferred digital currency, valued at approximately $16,847.47 at the time, from Individual Victim 3's account with Digital Currency Exchange A, with servers outside of Maryland.

f. On or about June 25, 2019, **MILLESON**, in Maryland, took unauthorized control of Individual Victim 4's account with Social Media Platform A, with servers outside of Maryland.

g. Beginning no later than on or about June 8, 2019, and continuing through at least in or about February 2020, **MILLESON**, in Maryland, registered at least ten different fraudulent internet domains with a registrar outside of Maryland. The domain names registered by **MILLESON** were designed to deceive others to believe they were associated with legitimate companies, including the Wireless Providers.

h. On or about October 9, 2019, **MILLESON**, in Maryland, registered "Fraudulent Domain B," a fraudulent internet domain, with a provider outside of Maryland, with a name designed to deceive others to believe it was associated with Wireless Provider B. The website hosted at the fraudulent domain was designed to steal the login credentials of legitimate users of Wireless Provider B's computer networks.

i. On or about January 27, 2020, **MILLESON**, in Maryland, caused a transfer of Bitcoin to a registrar outside of Maryland, to renew his ownership of Fraudulent Domain B. The fraudulent website hosted at Fraudulent Domain B continued to be active and accessible on the internet through at least in or about February 2020.

The Charges

26. On or about the dates set forth below, in the District of Maryland, and elsewhere, the defendants,

JORDAN K. MILLESON, and
KYELL A. BRYAN

each defendant charged in the counts listed below, for the purpose of executing the scheme to defraud described above, and attempting to do so, caused to be transmitted by means of wire communication in interstate commerce the signals and sounds, described below, each transmission constituting a separate count:

COUNT	DEFENDANT	DATE	WIRE TRANSMISSION
ONE	**MILLESON**	June 17, 2019	Registration of Fraudulent Domain A
TWO	**MILLESON**	June 25, 2019	Unauthorized access of Wireless Provider A's computer network using the credentials of Individual Victim 2
THREE	**MILLESON** **BRYAN**	June 25, 2019	Theft from Individual Victim 3's account with Digital Currency Exchange A
FOUR	**BRYAN**	June 26, 2019	Phone call to Baltimore County Police Department to "swat" **MILLESON**
FIVE	**MILLESON**	October 9, 2019	Registration of Fraudulent Domain B
SIX	**MILLESON**	January 27, 2020	Renewed Registration of Fraudulent Domain B

18 U.S.C. § 1343
18 U.S.C. § 2

COUNTS SEVEN AND EIGHT
(Unauthorized Access of a Protected Computer in Furtherance of Fraud)

The Grand Jury for the District of Maryland further charges that:

1. Paragraphs 1 through 25 of Counts One through Six are hereby incorporated by reference as though fully set forth herein.

2. On or about the dates listed below, each unauthorized access being a separate count, in the District of Maryland, and elsewhere,

JORDAN K. MILLESON, and
KYELL A. BRYAN

knowingly and with intent to defraud, accessed and attempted to access a protected computer, specifically, user accounts on the computer systems of Wireless Provider A and Digital Currency Exchange A, without authorization, and by means of such conduct furthered the intended fraud and obtained something of value, to wit: digital currency belonging to Individual Victim 3, held at Digital Currency Exchange A.

COUNT	DEFENDANT	DATE	COMPUTER SYSTEM	ACCOUNTHOLDER
SEVEN	**MILLESON**	June 25, 2019	Wireless Provider A	Individual Victim 2
EIGHT	**MILLESON BRYAN**	June 25, 2019	Digital Currency Exchange A	Individual Victim 3

18 U.S.C. §§ 1030(a)(4), (b) & (c)(3)(A)
18 U.S.C. § 2

COUNTS NINE AND TEN
(Intentional Damage to a Protected Computer)

The Grand Jury for the District of Maryland further charges that:

1. Paragraphs 1 through 25 of Counts One through Six are hereby incorporated by reference as though fully set forth herein.

2. On or about the dates listed below, each unauthorized access being a separate count, in the District of Maryland, and elsewhere,

JORDAN K. MILLESON,

knowingly caused the transmission of a program, information, code, and command, and as a result of such conduct intentionally caused damage without authorization, to protected computers, specifically taking over the listed users' accounts on the computer systems of the Social Media Platform A and Social Media Platform B:

COUNT	DATE	COMPUTER SYSTEM	ACCOUNTHOLDER
NINE	September 23, 2017	Social Media Platform B	Individual Victim 1
TEN	June 25, 2019	Social Media Platform A	Individual Victim 4

18 U.S.C. §§ 1030(a)(5)(A), (b), and (c)(4)(B)
18 U.S.C. § 2

COUNTS ELEVEN THROUGH FOURTEEN
(Aggravated Identity Theft)

The Grand Jury for the District of Maryland further charges that:

1. Paragraphs 1 through 25 of Counts One through Six are hereby incorporated by reference as though fully set forth herein.

2. On or about the dates listed below, in the District of Maryland, and elsewhere, the defendants,

JORDAN K. MILLESON,
and KYELL A. BRYAN

each defendant charged in the counts listed below, did knowingly transfer, possess and use and attempt to use, without lawful authority, a means of identification of another person, to wit: the defendants possessed and used the electronic account credentials of the individuals listed below, without lawful authority, during and in relation to Wire Fraud, Unauthorized Access of a Protected Computer in Furtherance of Fraud, and Intentional Damage to a Protected Computer in violation of 18 U.S.C. §§ 1343, 1030(a)(4), and 1030(a)(5)(A), as charged in the counts listed below:

COUNT	DEFENDANT	DATE	PERSON	COMPUTER SYSTEM	CHARGED COUNTS
ELEVEN	**MILLESON**	September 23, 2017	Individual Victim 1	Social Media Platform B	NINE
TWELVE	**MILLESON**	June 25, 2019	Individual Victim 2	Wireless Provider A	TWO & SEVEN
THIRTEEN	**MILLESON BRYAN**	June 25, 2019	Individual Victim 3	Digital Currency Exchange A	THREE & EIGHT
FOURTEEN	**MILLESON**	June 25, 2019	Individual Victim 4	Social Media Platform A	TEN

18 U.S.C. §§ 1028A(a)(1), (c)(4) and (c)(5)
18 U.S.C. § 2

COUNT FIFTEEN
(Wire Fraud Conspiracy)

The Grand Jury for the District of Maryland further charges that:

1. Paragraphs 1 through 25 of Counts One through Six are hereby incorporated by reference as though fully set forth herein.

2. On or about June 25 and 26, 2019, in the District of Maryland, and elsewhere, the defendants,

JORDAN K. MILLESON, and
KYELL A. BRYAN

and others known and unknown to the Grand Jury, did knowingly and willfully conspire, confederate, and agree to commit wire fraud in violation of 18 U.S.C. §1343, that is, to knowingly and willfully devise and intend to devise a scheme and artifice to defraud companies and individuals, and to obtain money and property, including funds in the form of digital currency, by means of materially false and fraudulent pretenses, representations, and material omissions, as described above, and for the purpose of executing and attempting to execute the scheme to defraud, did transmit and cause to be transmitted by means of wire and radio communication in interstate commerce, writings, signs, signals, pictures, and sounds.

18 U.S.C. § 1349

FORFEITURE

1. The allegations contained in Counts One through Fifteen are realleged and incorporated here for the purpose of alleging forfeiture.

2. Pursuant to Rule 32.2, Fed. R. Crim. P., notice is hereby given to the defendants that the United States will seek forfeiture as part of any sentence in accordance with 18 U.S.C. §§ 981(a)(1)(C), 982(a)(2)(B), and 1030(i), and 28 U.S.C. § 2461(c), in the event of the defendants' conviction under any of Counts One through Fifteen.

FORFEITURE OF CRIMINAL PROCEEDS

3. As a result of the offenses charged in One through Fifteen, the defendants,

JORDAN K. MILLESON, and
KYELL A. BRYAN,

shall forfeit to the United States any and all property constituting, or derived from proceeds obtained directly or indirectly as a result of such violations, and all interest and proceeds traceable thereto, including, but not limited to:

a. At least $16,847.47; and

b. All Bitcoin or other digital currency constituting or traceable to proceeds of the charged offenses.

FORFEITURE OF FACILITATING PROPERTY

4. As a result of the offenses charged in Counts Seven through Ten, the Defendants,

JORDAN K. MILLESON, and
KYELL A. BRYAN,

shall forfeit to the United States any and all personal property used, or intended to be used, in any manner or part, to commit, or facilitate the commission of, such violations, including, but not

limited to computers and other devices capable of storing digital information, internet domains, and websites.

SUBSTITUTE ASSETS

5. If any of the property described in this Superseding Indictment as being subject to forfeiture, as a result of any act or omission of the defendant,

a. cannot be located upon the exercise of 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 18 U.S.C. §§ 981 and 982, 21 U.S.C. § 853, and 28 U.S.C. § 2461, to seek forfeiture of any other property of the defendants up to the value subject to forfeiture.

18 U.S.C. §981(a)(1)(C)
18 U.S.C. §§ 982(a)(2)(A) and (B)
18 U.S.C. § 1030(i)
28 U.S.C. § 2461(c)

Robert K. Hur

Robert K. Hur
United States Attorney

A TRUE BILL

Date: 9-9-20

SIGNATURE REDACTED
Foreperson