IN THE CIRCUIT COURT OF THE ELEVENTH JUDICIAL CIRCUIT
IN AND FOR MIAMI-DADE COUNTY, FLORIDA

STATE OF FLORIDA)
) SS
COUNTY OF MIAMI-DADE)

FILED FOR RECORD
2024 JAN 29 AM 9:05

AFFIDAVIT IN SUPPORT OF ARREST WARRANT

Before me, Mindy S. Glazer, a Judge of the Circuit Court of the Eleventh Judicial Circuit in and for Miami-Dade County, Florida, personally appeared Detective Adrian Perez, ID No. 30-07486, of the Miami-Dade Police Department ("MDPD"), who being by me first duly sworn, deposes and says that there is probable cause to arrest:

Courtney Taylor Clenney (hereinafter "SUBJECT 1"), [redacted]

and

Kim Dewayne Clenney (hereinafter "SUBJECT 2"), [redacted]

and

Deborah Lyn Clenney (hereinafter "SUBJECT 3"), [redacted]

who, together as principals of one another along with other uncharged individual(s), did commit one (1) count of Unauthorized Access or Excessive Access to a Computer, Computer System, or Electronic Device of Christian Tobechukwu Obumseli, a Black Male with a date of birth of April 12, 1994 and/or his estate (hereinafter the "Victim"), a third-degree felony, in violation of Florida Statute § 815.06(2)(a), contrary to the form of the statute, in such cases made and provided, and against the peace and dignity of the State of Florida.

ASA [signature] Affiant AP Judge MSG

AFFIANTS' BACKGROUND

Your Affiant is Detective Adrian Perez, ID #7486, who has been a law enforcement officer with the Miami-Dade Police Department since January 2016 and is currently assigned to the Cybercrimes Bureau ("CCB"). Your Affiant is a federally deputized task force officer with the United States Secret Service's South Florida Cyber Fraud Task Force ("SFCFTF") and has been previously assigned to the Miami-Dade County State Attorney's Office Violent Gang/Cyber Strike Force. Your Affiant has a 4-year baccalaureate degree conferred by Florida State University in the field of Information Technology (I.T.) and holds multiple information technology certifications in various specializations including computer networking, cybersecurity, and computer server management. Additionally, Your Affiant has received continuous training in Cyber, Internet, and Social Media investigations from the Miami-Dade Public Safety Training Institute, National White Collar Crime Center ("NW3C"), National Computer Forensics Institute ("NCFI") and the SANS Institute.

Your Affiant's duties include the investigation of cyber related crimes, including cyber-attacks and intrusions, cyber-enabled fraud, cyber threats to critical infrastructure, dark web investigations, and undercover cyber operations. Additionally, Your Affiant has been trained to provide on-scene incident response to investigate and mitigate active network intrusions reported by victims. Your Affiant is familiar with the way computers, computer networks, and technology is utilized in the furtherance of crimes both at the state and federal levels. As a result of the above-mentioned training and experience, Your Affiant has previously prepared numerous subpoenas, court orders and search warrants and has worked closely with the Miami Dade State Attorney's Office Cybercrimes unit in previous investigations.

This affidavit is based upon information known personally to your affiant and information obtained from others who have investigated this matter and/or have personal knowledge of the facts herein. Your Affiant has participated in this investigation, spoken with other law enforcement detectives, and has reviewed documents and police reports related to this investigation. This affidavit is being submitted for the limited purpose of establishing probable cause and, therefore, does not include every aspect, fact, or detail surrounding this investigation.

FACTS IN SUPPORT OF PROBABLE CAUSE

Your Affiant was assigned as the lead investigator in the cybercrime documented under MDPD case number PD231219415622. The investigation was initiated following an

investigative referral by the State Attorney's Office to the Miami-Dade Police Department. MDPD, as the "Sherriff" of Miami-Dade County, has jurisdiction throughout Miami-Dade County, including crimes committed by inmates in its jails.

I. UNDERLYING CASE

Christian Obumseli (herein "Victim") was killed on April 3, 2022, because of an apparent stab wound inflicted upon him by Courtney Clenney (herein "SUBJECT 1") in their City of Miami apartment. Following the victim's killing, many of his belongings were taken from the apartment by unknown persons and have not been provided to his family, heirs, or estate. After the victim was killed, an investigation was conducted by the City of Miami and State Attorney's Office resulting in Subject 1's arrest and charging under Miami-Dade County Court case number F22014137. A search of Miami-Dade County records shows Subject 1 has been in Miami-Dade Corrections and Rehabilitation custody since August 26, 2022, under Miami-Dade jail number 220149337.

While Subject 1's case was proceeding, the City of Miami made several attempts to access Subject 1's cellular phone with no success (the device was locked with a five-digit passcode). To get Subject 1's cellular phone contents by other means, the City of Miami sought and received two warrants (hereinafter "iCloud Warrant 1" and "iCloud Warrant 2") for Subject 1's iCloud account ctc496@me.com. The City of Miami additionally sought the iCloud accounts of Kim Clenney (herein "SUBJECT 2") and Deborah Clenney (herein "SUBJECT 3") because of messages exchanged with Subject 1, known photographs taken of Subject 1 by Subject 3, and comingling of financial accounts by Subject 2.

Your affiant knows that an "iCloud" is a cloud-based storage and syncing system linked to Apple devices. By linking individual Apple devices to a particular iCloud account, certain contents of those devices can be automatically synchronized to/from the iCloud account and multiple Apple devices. Such content includes documents, photos, notes, and contacts. iCloud can also be used to locate lost or missing Apple devices and to remotely destroy data on such Apple devices. iCloud also allows the owner or user of a particular iCloud account to manage synchronized email, contacts, calendars, notes, reminders, photos, cloud storage, word-processing documents, spreadsheets, and presentations through a standard web browser. Changes made to the above-described resources in iCloud can then be automatically pushed to the owner or user's linked Apple devices.

iCloud warrant 1 was signed by the Honorable Judge Carmen Cabarga on February 2, 2023. iCloud warrant 1 was served on Apple, Inc., which complied by providing multiple voluminous download links on March 1, 2023. Downloads of the iCloud data were made, but not reviewed, due to the technical expertise required to review the material, the volume of the data, and the establishment of a "filter" protocol to prevent inadvertently locating attorney-client communications.

To address these issues, the State Attorney's Office learned that an MDPD digital forensics expert, Sgt. Sergio Cremisini (ID 30-7369), could download and process the data, filter out communications that needed excising, and provide a simplified reader for investigators to digest the data. To achieve this, however, Sgt. Cremisini would require a new "download link" as the original return links had already expired. Consequently, City of Miami investigators applied for, and received, iCloud Warrant 2 from the Honorable Judge Andrea Wolfson on November 3, 2023. iCloud warrant 2 was served on Apple, Inc., which complied by providing multiple voluminous download links on November 16, 2023. The download links were provided to Sgt. Cremisini, along with the original preserved downloads from iCloud warrant 1, at which time he processed the records into a digestible reader format. Regarding Subject 3's messages, the updated records of iCloud warrant 2 suggested that strings of text messages were missing or had been deleted. As a result of this inference, Subject 3's messages from iCloud warrant 1 were compiled for comparison. All "filtered" records were provided to the State Attorney's Office in December 2023.

II. CYBER CRIME INVESTIGATION

An initial review of Subject 3's messages prompted an investigative referral on December 18, 2023, from the State Attorney's Office to Your Affiant regarding the willful and knowing unlawful access of a computer. Following the referral, Your Affiant received a copy of the primary evidence including Subject 1's arrest warrant; iCloud warrant 1; iCloud warrant 2; the victim's cellular phone extraction, Subject 1's cellular phone extraction (Subject 1's iCloud revealed a possible password that unlocked Subject 1's cellular phone and allowed its extraction), and Subject 3's iCloud warrant returns.

Contained within Subject 3's iCloud warrant returns were backed up messages from her phone. Of pertinence here was a group chat that included herself, Subject 2, Frank Andrew Prieto (hereinafter "INDIVIDUAL 1"), Sabrina Puglisi (hereinafter "INDIVIDUAL 2"), Manuel Recio

(hereinafter "INDIVIDUAL 3"), and Pamela Corvalan (hereinafter "INDIVIDUAL 4). Individuals 1, 2, 3, 4 represent Subject 1 in her underlying case. Subjects 2 and 3 are not clients of Individuals 1, 2, 3, or 4 as defined by section 90.502. Subjects 2 and 3, as listed witnesses in Subject 1's underlying case, were subject to legal process and therefore could not be represented by Individuals 1, 2, 3, or 4. Accordingly, there is no attorney-client privilege contained within the messages. Additionally, because the conversations were sought or obtained to enable or aid the commission of a crime, there is no attorney-client privilege to the conversations.

Contained within the group chat, between both iCloud warrant returns, were 4,230 messages. For unknown reasons, Subject 3's iCloud warrant 2 messages began on May 17, 2023 while the last message in iCloud warrant 1 was January 19, 2023 - therefore leaving a period of approximately four months of messages unaccounted for. Included within the group chat were various discussions about the victim's laptop and how to access it. The first noted reference to the victim's laptop was made by Subject 2 on September 23, 2022 at roughly 8:45 p.m. Apparently in response to an earlier conversation about Subject 1 and discussions with her, Subject 2 wrote, "Forgot ask if she gave any ipotential passwords for the laptop." (All typographical errors in original; referenced times are in the Eastern time zone and were confirmed through known messages sent by Subject 2 to Subject 1 in the underlying case). Individual 1 replied on the same date at approximately 9:13, "Yes. Sabrina and I have a list. We will provide." Subject 2 replied immediately, "Thanks."

Several days pass with no conversation when Subject 2 messages the group chat on September 26, 2022, at approximately 4:25 p.m. writing, "Will you be sending the laptop PIN ideas so we can try them before you see her again?" in an apparent reference to accessing the victim's laptop using guessed passwords. Individual 1 replied on the same date at approximately 6:33 p.m., "Good evening guys. I have a couple that I can forward to you tomorrow." Subject 2 immediately replied, "Ok. Thanks." Several days pass with discussions about other matters when Subject 2 again raises the issue of passwords with the group. On September 29, 2022, at approximately 6:58 p.m Subject 2wrote "Are there any PIN/passwords we can try before you see her tomorrow?" Individual 2 replies shortly afterwards (approx. 7:03 p.m.), "She didn't have anything for me." Subject 2 replied at approx. 7:10 p.m., "Last Friday evening Frank indicated that there was a list. You may want to ask her again tomorrow." Individual 2 replied 38 minutes later (approx. 7:48) stating, "I'll ask her tomorrow." Subject 2 replied at approx. 8:04 p.m.,

"Thanks." Individual 1, apparently in response to Subject 2's multiple inquires for passwords, then began sending several back-to-back messages to the group chat at approx. 8:23 p.m. Individual 1 sent 6 messages with possible passwords and then, at approx. 8:24 p.m. wrote, "These were possible....was not sure about capitalization or spacing but there are the ones she could come up with." Individual 1 then sent a second message immediately afterwards saying, "I would try all together and mix some of the capitalization and see if we get lucky." Subject 2 replied 11 minutes later, "Ok. Thanks." About 23 minutes later, Subject 2 wrote: "Now I know that the PIN is actually a 4 digit number. Letters are not able to be entered. Only numbers. Sabrina, please ask her for options." The following day (September 30, 2022, at approx. 3:57 p.m.), completely out of context for the messages, Subject 2 wrote: "Hell yeah! That PIN worked!" Individual 4 "Loved" the message about 3 minutes later. Individual 1 replied to Subject 2's message at approx. 4:02 p.m. writing, "Kim. Hold off on going through the computer please. I don't want to turn you into a witness just yet if you find something useful." Individual 1 furthered, "But that is great news and makes this easie." Subject 2 replied a moment later, writing, "Ok. Understood."

A discussion was then had regarding custody of the laptop, whether Subject 2 should ship the victim's laptop to Individual 1. Individual 1 discussed how shipment might be possible, but he would like to speak with a computer consultant. Individual 1 then added he would be in Dallas the following week and may want to pick up the victim's laptop "in the abundance of caution just in case." Subject 2 acknowledged and Individual 1 furthered, "When it comes to potential evidence, we always have to consider 'chain of custody' issues and don't necessarily want to take risk something gets 'lost' in mail. But hang tight. We will make a decision by Monday." Subject 2 again acknowledged. Individual 2 then sent another message, writing, "Also, as I'm sure you guessed by me prior text, we don't want you accessing files because the State Attorneys could request their own independent analysis of the hard drive and accuse you of creating or modified files. That's why I wanted to put a quick pause on that. Obviously I know you would not do that but we want to maintain that credibility." Subject 2 replied, "I had barely opened it and was starting to poke around, but we started a video call so I stopped. Never opened a file, so I didn't see anything." Individual 1 replied, "Sounds good."

Several days passed without discussion about the victim's laptop, though other discussions about meetings were had. Subject 2 sent a message on October 4, 2022 at approx.

4:58 p.m., writing: "I'd also like for you to have the laptop soon, so you can see if there's anything of use to us on it." Several more messages about meetings between Subjects 2 and 3 and the Individuals are exchanged over several days without reference to the victim's laptop. Subject 3 then messages the group chat at approx. 12:09 p.m. on October 6, 2022, "I will be making the drive to Dallas tomorrow to drop off the laptop. I am hoping that Morgan will come with me." This is a reference to Individual 1's travel to Dallas discussed above. It should also be noted that Subjects 2 and 3 reside in Austin, Texas, several hours away from Dallas. Individual 1 replied 2 hours later, "Ok. Sounds Great. The earlier the better. Hoping to catch an earlier flight back to Miami but drive safe and see you tomorrow. Look forward to meeting Morgan if she comes with you." There were then several discussions that continued into the next day about their anticipated arrival time. On October 7, 2022, more messages coordinating the unauthorized transfer of the victim's laptop were exchanged between Subject 3 and Individual 1, which included location information, travel time, travel updates, and estimated time of arrival. Several hours later - October 7, 2022, at approx. 4:29 p.m. – Individual 1 wrote to the group chat, "Hey Deborah. Good seeing you today. I forgot to have you sign a property receipt for turning over the laptop. I will get one to you next week to sign. Thank you for brining it to Dallas area." Subject 3 immediately replied, "Ahhh. Ok. And you're welcome."

The messages then do not discuss victim's laptop again for several months. Noting again there are no records from January 19, 2023, until May 17, 2023 – the next time the victim's laptop is discussed is on July 8, 2023. Individual 1 sent a message to the group chat at approx. 6:58 p.m., writing, "Good evening everyone. Mike Haas (IT expert) now has possession of all the electronics we need him to evaluate, clone, and run searches on. I did not have the password for the suspected Obumseli Asus laptop handy. Does anyone have that readily available? Please send when you can." "Mike Haas" was later identified as Michael Walter Haas (W/M, DOB: 02/21/1984, hereinafter "Individual 5"), an individual with an Information Technology company named "Pivotal IT Consulting, LLC" that has a principal address in Miami, Florida. The following morning, at approx. 9:49 a.m., Subject 2 replied, "I think the code to the laptop is 0412." It should be noted the victim's birthday is April 12 (04/12). Several days with unrelated conversations occurred until the next – and last known – discussion about the victim's laptop occurred 16 days later on July 25, 2023 at 12:38 p.m. Subject 2 wrote, "Courtney was asking

about the visit schedule this week. Also, do we have any updates on the video and the laptop? Since it has been 7 weeks since the last zoom meeting, possible we can set up another soon."

Your Affiant made contact with Kimberly Wald, Esq. (hereinafter "Attorney Wald") on Friday, January 12, 2024. Attorney Wald is counsel for the victim's estate. Ms. Wald informed your affiant that the victim's estate has never received the victim's property from anyone including Subjects 1, 2, or 3 or Individuals 1, 2, 3, 4, or 5. Attorney Wald further advised the victim's estate has never given permission to anyone including Subjects 1, 2, or 3 or Individuals 1, 2, 3, 4, or 5 to possess or keep the victim's belongings. Finally, Attorney Wald advised the victim's estate or family has never provided consent or authorization to anyone including Subjects 1, 2, or 3 or Individuals 1, 2, 3, 4, or 5 to access the victim's laptop.

III. CRIMES AGAINST USERS OF COMPUTERS

In Florida, "[a] person commits an offense against users of computers, computer systems, computer networks, or electronic devices if he or she willfully, knowingly, and without authorization or exceeding authorization [a]ccesses or causes to be accessed any computer, computer system, computer network, or electronic device with knowledge that such access is unauthorized or the manner of use exceeds authorization." §815.06(2)(a), Fla. Stat. This offense is a third-degree felony.

Based on the totality of the circumstances, from September 23, 2022 to at least July 25, 2023, the Subjects collectively along with Individuals 1 and 2 as principals of one another, accessed or caused to be accessed the victim's laptop with knowledge that such access was unauthorized or the manner exceeded authorization because none of the Subjects or Individuals sought authorization from the victim (who could not authorize such access because he is deceased), the victim's estate, or the victim's representative. This is evidenced by the clear attempts to evade discussions about the victim's laptop via monitored jail calls, willfully enlisting Individuals 1 and 2 to obtain possible access codes in person from Subject 1 in the Miami-Dade County jail, and the unlocking of the laptop by Subject 2. Additionally, Subject 3 transported the device from Austin to Dallas, Texas, where Individual 1 took possession of the victim's laptop – ultimately providing it to Individual 5 in the city of Miami for unlawful access. (At this juncture, there is no evidence Individual 5 knew he could not access the victim's laptop).

Criminal intent is apparent throughout the messages, such as: Subject 2's rush to get the victim's laptop to Individual 1 so he could "see if there's anything of use to us on it"; Subject 2's

constant inquiring of the victim's laptop when he first accessed it in October 2022; Subject 3's hand delivery of the victim's laptop to Individual 1; Individual 1's delivery of the laptop to Individual 5.

Furthermore, knowledge of ownership of the laptop can be inferred by mention of Individual 1 on the group thread referring to the device as "the suspected Obumseli Asus laptop."

IV. CONCLUSION

Accordingly, based on the totality of the circumstances, Your Affiant has probable cause to arrest: **Courtney Taylor Clenney ("SUBJECT 1"), Kim Dewayne Clenney ("SUBJECT 2"), and Deborah Lyn Clenney ("SUBJECT 3")** who, together as principals of one another along with other uncharged individual(s), did commit one (1) count of Unauthorized Access or Excessive Access to a Computer, Computer System, or Electronic Device of Christian Obumseli and/or his estate, a third-degree felony, in violation of Florida Statute § 815.06(2)(a), contrary to the form of the statute, in such cases made and provided, and against the peace and dignity of the State of Florida.

AFFIANT
Detective Adrian Perez, ID # 7486
Miami-Dade Police Department

SWORN TO AND SUBSCRIBED BEFORE ME, THIS 26th DAY OF January 2024.

Circuit Court Judge
Eleventh Judicial Circuit of Florida

MINDY S. GLAZER
CIRCUIT COURT JUDGE

STATE OF FLORIDA, COUNTY OF DADE
I HEREBY CERTIFY that the foregoing is a true and correct copy of the original on file in this office. 1/29/24 AD 20____
Clerk of Circuit and County Courts
Juan Fernandez-Barquin
Deputy Clerk 323831

ASA ____ Affiant ____ Judge ____