UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
JACKSONVILLE DIVISION

UNITED STATES OF AMERICA

v. CASE NO. 3:20-cr-26-BJD-LLL

SAMUEL ARTHUR THOMPSON

UNITED STATES' RESPONSE IN OPPOSITION TO DEFENDANT'S *PRO SE* MOTION TO SUPPRESS AND REQUEST FOR *FRANKS* HEARING

The United States of America files this response in opposition to Defendant's *Pro Se* Motion to Suppress and Request for Franks Hearing, (Doc. 132, hereinafter, "Defendant's Motion"), which was filed on October 3, 2022. Defendant has not made the threshold showing that would entitle him to a *Franks* evidentiary hearing, and none should be granted. Furthermore, the other grounds for relief that defendant asserts in his motion – that the search warrant affidavit failed to set forth probable cause to believe a crime had been committed, that the warrant was not sufficiently particular and was overbroad, that the search exceeded the scope of the warrant, and that the warrant was executed in an unreasonable manner – are both factually and legally unfounded. His motion should therefore be denied.

PERTINENT FACTS

As described in Special Agent (SA) Frank Norris's affidavit, which is attached as Exhibit A to Defendant's Motion, the initial investigation of this case arose after the Jacksonville Jaguars reported to the Federal Bureau of Investigation (FBI) in

2018 that defendant had been accessing a secure computer network located at the Jaguars' stadium during the 2018 National Football League (NFL) season. Doc. 132-1 ¶¶ 5-7. Defendant previously had been employed as a contractor for the Jaguars with responsibility for the video board network, known as a "Jumbotron," but his contract was not renewed after the Jaguars learned of defendant's criminal record. *Id.* ¶ 7.

The network intrusions that SA Norris was investigating had occurred well after the expiration of defendant's contract with the Jaguars, on September 16, 2018, November 18, 2018, and December 2, 2018. *Id.* ¶ 9(a). SA Norris described that the network intrusions "resulted in the inability for the video board system operators to display the desired content," which SA Norris characterized as a form of denial-of-service (or "DoS") attack. *Id.* ¶ 9(b). The affidavit explained that "[a] DoS attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor." *Id.* SA Norris described that the Jaguars' investigation revealed that the network intrusions and outages had been the result of a device named MIRA9120 sending commands. *Id.* ¶ 9(c). A review of MIRA9120 revealed that remote access software called TeamViewer had been installed on MIRA9120, but the user who had installed TeamViewer on MIRA9120 had disabled connection logging. *Id.* ¶ 9(e).

SA Norris described in his affidavit that on December 3, 2018, the Jaguars disconnected MIRA9120 from the video board network and enabled connection

logging in an attempt to discover any new connections made during an upcoming event (which was an NFL game) on December 16, 2018. *Id.* ¶ 10. On December 16, 2018, the TeamViewer log file recorded that a user logged into MIRA9120 using a particular IP address. *Id.* ¶ 11(b). A subpoena to Comcast Cable showed that that IP address was assigned to Jean Louise Puckett at 113 Marsh Island Circle, St. Augustine, Florida. *Id.* ¶ 14. This address was also defendant's residence. *Id.* ¶¶ 15-16. FBI's investigation also revealed that a Dropbox.com account that was attributed to defendant was logged in on MIRA9120 during the same timeframe that TeamViewer was installed on MIRA9120. *Id.* ¶¶ 11(a), 13.

Based on this investigation, on July 11, 2019, SA Norris obtained a federal warrant to search the 113 Marsh Island Circle residence. *See* Case. No. 3:19-mj-1251-MCR. The Attachment B to the warrant authorized the seizure of "[c]omputers and electronic storage media" and further authorized the search of any computers or electronic storage media seized for a specific list of items of evidentiary value enumerated in paragraph 4 of Attachment B.

On July 17, 2019, federal agents executed the warrant. Defendant was at the residence at that time. Defendant's iPhone 7 (which meets the definition of a computer authorized to be seized by the warrant) was in plain view in his hand while he was inside of the residence and was seized by SA JulianCarl Slaughter. Approximately 20 other computers or electronic storage media also were seized from the residence. Defendant informed the agents that he possessed another computer

in an off-site storage unit and consented to the seizure and search of that computer without limitation. Agents also seized a firearm as contraband because defendant is a convicted felon. Upon completing the search, agents left a copy of the warrant with its attachments on a table inside of the residence and took a photo of it.

Defendant fled to the Philippines, via the Republic of Korea, on July 26, 2019. Defendant failed to report his international travel in violation of the Sex Offender Registration and Notification Act (SORNA). Defendant had also traveled to the Bahamas earlier in July 2019 without updating his sex offender registration.

While searching the seized computers, agents identified child sex abuse material on defendant's iPhone 7, on the computer seized (by consent) from the storage unit, and on a hard drive located inside of the residence. The FBI sought and obtained additional warrants authorizing the search of each seized electronic storage medium (other than the computer in the storage unit, for which agents had consent) for evidence related to child sex abuse material.

Defendant is charged in a Superseding Indictment with six counts: possession of child sex abuse material (Count One); receipt of child sex abuse material (Count Two); causing transmissions of commands to protected computers without authorization (Count Three); a SORNA violation related to the defendant's travel to the Bahamas (Count Four); possession of a firearm by a convicted felon (Count Five); and a SORNA violation related to defendant's travel to the Republic of Korea and the Philippines (Count Six). Doc. 39.

MEMORANDUM OF LAW

I. The affidavit demonstrated probable cause that a violation of Section 1030 had been committed

Defendant submits that SA Norris's affidavit did not state probable cause to believe there was a violation of Section 1030, which was the statutory authority for the warrant. Doc. 132 at 5-8. Defendant submits that, with regard to Section 1030(a)(2)(C), there was no probable cause in the affidavit that defendant "obtained information" from the protected computer that he accessed without authorization. *Id.* at 8. Defendant ignores the expansiveness of the term "obtain information." Congress intended this term to include the mere viewing of information. *See* S. Rep. No. 99-432 at 6 ("Because the premise of [Section 1030(a)(2)] is privacy protection, the Committee wishes to make clear that 'obtaining information' in this context includes mere observation of the data."); *see also* Eleventh Circuit Pattern Jury Instruction O42.2 Annotations and Comments ("The Senate Judiciary Committee emphasized that 'obtains information' in this context includes mere observation of the data."). SA Norris established probable cause for this element by showing that defendant had repeatedly accessed a protected computer without authorization – and by ready inference, had observed information on that computer.

With regard to Section 1030(a)(5)(C), defendant submits that there is no probable cause in the affidavit that defendant "cause[d] loss" as a result of his unauthorized access to a protected computer. *Id.* Defendant is incorrect. "Damage" is defined in Section 1030 to mean "any impairment to the integrity or

availability of data, a program, a system, or information" and "loss" is defined to mean "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(8) & (11). SA Norris described in his affidavit that, according to the Jaguars, during the intrusions "the video boards had experienced an outage from their standard operating design," and "the outage resulted in the inability for the video board system operators to display the desired content." Doc. 132-1 ¶ 9(a) & (b). Furthermore, SA Norris's affidavit establishes that the victim company is an NFL team, that the intrusions resulted in the inability of the team to operate its jumbotron during three separate NFL games, and that the team had conducted an internal investigation to determine the origin of the outages. *See id.* ¶¶ 5, 9. These facts established probable cause that the attacks caused damage and loss to the Jaguars.

In short, SA Norris established probable cause to believe that defendant had violated at least two subsections of Section 1030. The magistrate judge, upon reviewing the affidavit, found probable cause to believe that evidence of these violations would be found in defendant's residence, including computers inside of the residence. There is no reason to question the judgment of the magistrate judge who issued the warrant, but even if this Court were to determine that there was not

probable cause, the executing agents were entitled to rely on it in good faith. *United States v. Leon*, 468 U.S. 897 (1984); *United States v. Taylor*, 935 F.3d 1279, 1288-93 (11th Cir. 2019). There is no basis for suppression.

II. Defendant is required to make a substantial preliminary showing of entitlement to a *Franks* evidentiary hearing, which he has not done.

Defendant argues that he is entitled to an evidentiary hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), to probe the validity of the residential search warrant. Defendant must make "an offer of proof" as part of his substantial preliminary showing of entitlement to an evidentiary hearing and therein must demonstrate "that (1) the affiant deliberately or recklessly included false statements, or failed to include material information, in the affidavit; and (2) the challenged statement or omission was essential to the finding of probable cause."[1] *United States v. Arbolaez*, 450 F.3d 1283, 1293 (11th Cir. 2006). As the Eleventh Circuit has explained, "the substantiality requirement is not lightly met," and

> [t]o mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by a clear offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained.

[1] Defendant submits that "[i]mportantly, a substantial preliminary showing does not require 'clear proof' of the allegations of deliberate falsehood or of reckless disregard for the truth," Doc. 132 at 9 (citing *United States v. Williams*, 477 F.3d 554, 558 (8th Cir. 2007)). The United States submits that the standards set by Eleventh Circuit control.

Arbolaez, 450 F.3d at 1294 (quoting *Williams v. Brown*, 609 F.2d 216, 219 (5th Cir. 1979) (in turn quoting *Franks*, 438 U.S. at 171)). Absent an affidavit or sworn statement alleging that the affiant knowingly or recklessly included false statements, defendant is not entitled to an evidentiary hearing. *United States v. Flowers*, 531 F. App'x 975, 981 (11th Cir. 2013) (upholding denial of *Franks* hearing where defendant "provided no evidence that established [the affiant] either intentionally or recklessly omitted these facts" and noting that "the *Franks* Court identified 'affidavits or sworn or otherwise reliable statements of witnesses'" as examples of supporting proof); *United States v. Leach*, 498 F. App'x 915, 917 (11th Cir. 2012) (defendant must support allegations of falsity "by an offer of proof, including affidavits or sworn or otherwise reliable statements of witnesses"); *United States v. Cha*, 431 F. App'x 790, 796 (11th Cir. 2011) (no error in denial of *Franks* hearing where attacks on the affidavit "were conclusory and unsupported by any proof"); *Arbolaez*, 450 F.3d at 1294 (defendant "failed to make the necessary 'substantial preliminary showing,'" and it was therefore not error for the district court to have denied a *Franks* hearing, where "[t]here [was] no affidavit or otherwise sworn statement"); *United States v. Haimowitz*, 706 F.2d 1549, 1556 (11th Cir. 1983) (*Franks*-based suppression motion must be accompanied by an offer of proof that the affiant intended to mislead the magistrate judge). Where the disputed information came from an informant, "the defendant must show that it is the agent, and not the informant, who has made the misrepresentations." *United States v. Novaton*, 271 F.3d 968, 988 (11th Cir. 2001);

United States v. De Aza, 825 F. App'x 709, 711 (11th Cir. 2020) ("[A] defendant may impeach only the affiant's statement, not the informant's statement." (citing *Novaton*, 271 F.3d at 986)). Allegations advanced in a motion for a *Franks* hearing, unless supported by an affidavit or other proof, will not contribute to defendant's required "offer of proof." *United States v. Underwood*, No. 8:11-cr-95-T-26TBM, 2011 WL 2036498 (M.D. Fla. May 24, 2011) ("[T]he allegations advanced by Defendant's attorney, without more, cannot be considered by the Court in making up for" the lack of "affidavits or reliable witness statements").

If defendant is able to establish the first prong of *Franks* – that is, that there were deliberate or reckless misrepresentations or omissions in the affidavit – he still must establish that absent those misrepresentations or omissions there would not have been probable cause. *Leach*, 498 F. App'x at 917 (citing *Novaton*, 271 F.3d at 987). "That is the test of materiality, and materiality is essential no matter how deliberate or reckless the misrepresentations were." *Novaton*, 271 F.3d at 987. "When assessing whether the alleged false statements and omissions were material, the trial court is to disregard those portions of the affidavit which the defendant has shown are arguably false and misleading." *De Aza*, 825 F. App'x at 711 (quoting *United States v. Barsoum*, 763 F.3d 1321, 1328-29 (11th Cir. 2014)). Defendant is entitled to a hearing only if he can "show that, 'absent those misrepresentations or omissions, probable cause would have been lacking.'" *Id.* (quoting *Barsoum*, 763 F.3d at 1329, and citing *Novaton*, 271 F.3d at 986).

Defendant's motion for a *Franks* hearing is insufficient for several reasons. First, defendant fails to offer any proof for most of his assertions, and much of the proof he does offer actually refutes his assertions. Second, defendant fails to demonstrate that any purported inaccuracies in SA Norris's affidavit were deliberately or recklessly false. Third, even if the Court assumed that every fact defendant asserts is false is in fact false, and even if the court were to assume – without any offer of proof – that these false representations and omissions were made deliberately or recklessly, defendant still is not entitled to an evidentiary hearing because probable cause still would have existed for the search warrant.

A. Defendant has failed to support his assertions with a sufficient offer of proof.

Beginning on page 9 of Defendant's Motion, he makes several claims of falsity in SA Norris's affidavit. The *only* way in which defendant supports these assertions is by attaching several exhibits, none of which supports that there was falsity or any material omission. *See* Doc. 132-1 through 132-10. Defendant asserts the following were false or omitted from SA Norris's affidavit:

1. **Defendant submits that, after his contract with the Jaguars ended, he "maintained authorized access to the subject network and servers through his continued relationship with the City of Jacksonville through SMG" and that this fact was omitted from SA Norris's affidavit.** Doc. 132 at 9. In support, defendant cites two documents as proof of his claim – first, he attaches the contract between himself and the Jacksonville Jaguars (Exhibit E). This contract

states that it "shall continue until March 31, 2018" unless it was "earlier terminated in accordance with the terms hereof." Doc. 132-5 ¶ 1. As stated in SA Norris's affidavit, the information he received was that "THOMPSON was no longer employed" by the Jaguars as of February 23, 2018, because the Jaguars chose to terminate the contract. Doc. 132-1 ¶¶ 6-7. This is consistent with the information in SA Slaughter's report, which defendant attached as Exhibit F, which states that the Jaguars informed the FBI that "THOMPSON was relieved of his employment with [the Jaguars] on or about February 23, 2018." Doc. 132-6 at 2. Defendant secondly cites to SA Slaughter's report, which contains a typo causing it to read "THOMPSON did have authority to access the [Jaguars] networks once he was terminated." Doc. 132-6 at 3.[2] It is clear from the rest of the report that Defendant did *not* have authorized access to the Jaguars' systems at the time of the attacks. *See* Doc. 132-6 at 2 ("THOMPSON Utilizing the Team viewer application . . . made unauthorized access to the [Jaguars] video board network . . ."); *id.* at 3 ("THOMPSON conducted the unauthorized access denial of service attacks on three occasions[.]"); *id.* at 4 (discussing potential prosecution of "the network intrusion conducted by THOMPSON"). Even if it were the case that defendant continued to have access to the Jaguars' computer systems until March 31, 2018, the latest date on which his contract was set to expire, it is plain that defendant did not have authorized access months later, when the intrusions occurred. Defendant has not

[2] SA Slaughter has amended his report to correct this typo.

made a sufficient offer of proof to support his contention that he continued to have authorized access to the Jaguars' computer systems after he was terminated, and in fact, the documents attached by defendant show that he did not.

2. **Defendant submits that it was omitted from SA Norris's affidavit that "it was an anonymous letter addressed to Jaguar Senior Staff that prompted the decision not to renew Mr. Thompson's contract."** Doc. 132 at 10. Defendant states that the anonymous letter, which he attaches as Exhibit G, shows that there were "employees within the Jaguar organization [who] had animosity toward" him. *Id.* Defendant asserts that this "could have influenced the magistrate's determination of probable cause in weighing the credibility of the evidence provided to the agent" without specifying how this information could possibly have swayed the magistrate judge. Doc. 132 at 11. While the anonymous letter is not specifically described in SA Norris's affidavit, he does describe that defendant did not inform the Jaguars of his status as a convicted sex offender, and that the company "chose not to renew THOMPSON's contract after learning" that information. Doc. 132-1 ¶ 7. In any event, it is clear that the FBI conducted its own investigation and corroborated the information that had been provided by the Jaguars.

3. **Defendant submits that it was omitted from SA Norris's affidavit that "the Jaguars did not disclose to Mr. Thompson they were aware he was a registered sex offender and did not disclose to Mr. Thompson this was the**

reason his contract was not being renewed." Doc. 132 at 11. Again, defendant submits that this knowledge would have swayed the magistrate judge's probable cause determination because the magistrate judge "did not know Mr. Thompson believed he was leaving on good terms with the Jaguars, and that future engagement with the organization was possible." *Id.* Defendant does not attempt to explain how this could have impacted probable cause. In reality, this information only provides a motive for defendant's actions (that is, that he conducted the intrusions with the hope that he would be re-hired to fix the computers).

4. **Defendant disputes whether his last date of employment for the Jaguars was February 23, 2018, or March 31, 2018.** Doc. 132 at 12. Defendant cites as proof his contract, attached as Exhibit E, which he states SA Norris had possession of. *Id.* As described above, the contract on its face provides that it expired on March 31, 2018, "unless earlier terminated." Doc. 132-5 ¶ 1. SA Slaughter's report documents that the Jaguars informed the FBI that "THOMPSON was relieved of his employment with [the Jaguars] on or about February 23, 2018." Doc. 132-6 at 2. Defendant does not attempt to specify how this would impact the probable cause determination, except to contend that his access on February 23, 2018, was legitimate.

5. **Defendant complains that it was omitted from SA Norris's affidavit that defendant was working to prepare for the Monster Truck Jam at the stadium on February 23, 2018.** Doc. 132 at 13. Defendant supports his claim that

he was performing legitimate work on February 23, 2018, by attaching text messages extracted from his phone. Doc. 132-8. Defendant again does not articulate how this information could have impacted the probable cause determination.

6. **Defendant complains that it was omitted from SA Norris's affidavit that the Team Viewer account he used to conduct the intrusions was his personal Team Viewer account and could not have been terminated by the Jaguars.** Doc. 132 at 15. Defendant offers no proof of this assertion, nor does he attempt to explain how the information could have impacted probable cause, if true.

7. **Defendant contends that SA Norris made a false statement in paragraph 9(b) of his affidavit when he stated that the Jaguars were unable to replicate the issue with the video boards.** *Id.* Defendant ignores that paragraph 9 of SA Norris's affidavit summarizes "documents of the [Jaguars'] investigation into the incident" that were provided to SA Norris "[o]n December 10, 2018," describing investigation by the Jaguars that occurred on December 3, 2018. Doc. 132-1 ¶ 9. That is more than one month before the January 16, 2019, email that defendant attaches as proof. Doc. 132-9. Just because at some later date the Jaguars were able to replicate the issue does not render the summary of the investigation at an earlier point in time false. There is no inconsistency here or misrepresentation.

8. **Defendant submits that SA Norris omitted from his affidavit in paragraph 9(f) that the Jaguars had removed Team Viewer software from its computers "sometime *after* Mr. Thompson installed it on February 23, 2018."**

Doc. 132 at 15. Defendant attaches as proof an email thread between the FBI and the Jaguars in which the Jaguars state that Team Viewer was "removed from all known systems after February 25th" but that the exact date was unknown. Doc. 132-9 at 3. Defendant does not explain how this information could have impacted probable cause, and in any event, it is consistent with what SA Norris stated in his affidavit. Doc. 132-1 ¶ 9(f).

9. **Defendant takes issue with SA Norris describing the attack as a "denial-of-service" attack because, according to defendant "[i]n no conceivable way could this be construed as a denial-of-service attack."** Doc. 132 at 16. SA Norris's affidavit described the nature of the network intrusion and its result. *See generally* Doc. 132-1 ¶ 9 (describing the attack and defining a denial-of-service attack as occurring "when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor"). Defendant's submission of a differing definition of a denial-of-service attack and claim that what he did was *not* a denial-of-service attack is a red herring. It is irrelevant to the finding of probable cause whether or not it was a "denial-of-service attack" (it was) as that is not a term of art in Section 1030. Defendant makes no effort to articulate how SA Norris's accurate description of his attack as a denial-of-service attack somehow impacted the magistrate judge's finding of probable cause.

10. **Defendant submits that SA Norris mischaracterized the nature of the MIRA9120 server.** Doc. 132 at 17. Defendant submits that, rather than

being a decommissioned or "rogue" server, MIRA9120 "is a backup Abekas Mira server, installed after the inaugural NFL season with the new video boards" and could be used to "replace any one of the six active Abekas Mira's in the event of a failure during an event. *Id.* As reflected in defendant's Exhibit F, the Jaguars informed the FBI that MIRA9120 was a "rogue workstation" that was not set up in the "standard configuration." Doc. 132-6 at 3. Defendant makes no effort to support his contention with an offer of proof, nor to explain how it could impact probable cause. In any event, SA Norris reasonably relied on the information conveyed by the Jaguars to the FBI.

These purported inaccuracies and omissions represent the full extent of defendant's "offer of proof" in support of his request for a *Franks* evidentiary hearing. As described above, many of these contentions are utterly without any offer of proof whatsoever, and others (for example, the typo on which he lays one of his claims) demonstrate that defendant's alternative facts are inaccurate. Defendant has not met the first prong of *Franks* because he has failed to support with any offer of proof several of the facts that he argues were omitted or misrepresented. More critically, he does not advance even a bald allegation that SA Norris made *any* deliberate or reckless misrepresentations in his affidavit. *Arbolaez*, 450 F.3d at 1294 (defendant "failed to make the necessary 'substantial preliminary showing'" where "[t]here [was] no affidavit . . . alleging that [the affiant] knowingly or recklessly included false statements"). This is fundamental, because even "conclusory allegations of

negligence or innocent mistakes are insufficient." *Leach*, 498 F. App'x at 917; *see also United States v. Whyte*, 928 F.3d 1317, 1333 (11th Cir. 2019) ("Omissions made negligently or because of an innocent mistake are insufficient to warrant suppression of the evidence.").

Moreover, even assuming that all of defendant's factual assertions are true, to the extent that there were factual inaccuracies in the affidavit, those portions of the affidavit were attributed by SA Norris to information that was provided to him by the Jaguars and upon which SA Norris reasonably relied. *See, e.g.*, SA Norris Aff. ¶¶ 6-10 (describing information contained in the affidavit that was provided to SA Norris by the Jaguars regarding their investigation). Documents that defendant attaches to his motion only reinforce that SA Norris accurately represented in his affidavit information that had been provided to him by the Jaguars. SA Norris sufficiently corroborated the reporting by the Jaguars through an independent review of an image of the MIRA9120 hard drive that was conducted by an FBI computer scientist as well as subpoena-based investigation that linked the network intrusions to defendant and his residence. SA Norris Aff. ¶¶ 11-14; 16. Thus defendant has not carried his burden for the additional reason that he has not shown that "it is the agent, and not the informant" who made the purported misrepresentations. *Novaton*, 271 F.3d at 988.

For these reasons, defendant has failed to meet the first prong of *Franks* and is not entitled to an evidentiary hearing solely on that basis. Although there is no need

for the Court to look further in denying defendant's request for an evidentiary hearing, defendant also fails to meet the threshold set by the second prong of *Franks*.

B. Under the second prong of *Franks*, defendant is not entitled to an evidentiary hearing because probable cause existed regardless of the truth or falsity of the facts he now disputes.

Giving defendant the benefit of the doubt, and assuming that he *could* make the necessary showing under the first prong of *Franks*, he still would not be entitled to an evidentiary hearing because the facts that he disputes are irrelevant to the finding of probable cause.

As described in SA Norris's affidavit, the network intrusions he was investigating occurred during events hosted by the Jaguars on September 16, November 18, and December 2, 2018. Doc. 132-1 ¶ 9. FBI set up a sting on December 16, 2018, to attempt to capture any logins via TeamViewer to MIRA9120. *Id.* ¶¶ 10-11. During the sting, the TeamViewer software logged a connection from a user with account number 1118559964. *Id.* ¶ 11(b)(ii). A subpoena to TeamViewer showed that account 1118559964 had logged into MIRA9120 five times, most recently using an IP address that was attributed to defendant's residence. *Id.* ¶¶ 11(b)(ii) & 14. FBI's initial investigation also revealed evidence that defendant was the individual who had installed TeamViewer on MIRA9120 on February 23, 2018, which defendant acknowledges in his motion. *See* Doc. 132 at 15 ("TeamViewer had been removed from all of the devices sometime *after* Mr. Thompson installed it on February 23, 2018.").

Defendant now seeks to waste this Court's time by asking it to conduct an evidentiary hearing to quibble over facts that are entirely irrelevant to the existence of probable cause in the affidavit. Regardless of whether defendant's last day with the Jaguars was February 23, or March 31, 2018, whether defendant continued to have some level of legitimate access to the computers via his contractual employment with SMG, whether the Jaguars told him the real reason his contract was not renewed, whether certain employees of the Jaguars harbored animosity toward defendant, whether defendant installed Team Viewer on MIRA9120 for legitimate reasons in connection with the Monster Truck Jam, whether defendant's Team Viewer account was his personal account, and whether MIRA9120 was "rogue" or legitimate, the affidavit set forth probable cause that the defendant's access to the computers controlling the video boards via MIRA9120 during events put on by the Jaguars (not SMG) in September, November, and December 2018 was unauthorized. Defendant does not contend that he had authority to access the video boards in late 2018 – when the attacks occurred. Moreover, SA Norris's affidavit set forth probable cause to believe that the network intrusions on September 16, November 18, and December 2, 2018, were malicious and not legitimate, in that they "resulted in the inability for the video board system operators to display the desired content." Doc. 132-1 ¶ 9(b).

Defendant misses the mark by focusing exclusively on whether he had legitimate access to MIRA9120 in February-March 2018 and whether he had a

legitimate reason for installing software on MIRA9120 on February 23, 2018. Even crediting every claimed misrepresentation or omission as true – and also inferring without basis that those purported misrepresentations or omissions were deliberately or recklessly made by SA Norris – there would be no impact on probable cause, because the unlawful intrusions occurred six months or more after defendant's contractual employment for the Jaguars had been terminated. In other words, these purported misrepresentations and omissions are immaterial to probable cause.

III. The issued warrant was sufficiently particular and not overbroad

Defendant submits that "[t]he warrant in this case lacked particularity and was overbroad because it failed to sufficiently specify and limit the evidence sought." Doc. 132 at 19. Impliedly, defendant believes that agents should only have been authorized to search for documents related to the specific dates of the intrusions, and limited on those dates specifically to evidence of defendant's use of the TeamViewer application to remotely access the MIRA9120 server. *See id.* Defendant cites no authority to support his argument.

In fact, the law is to the contrary. For example, in *United States v. Richards*, the court reasoned that "[o]ne would not ordinarily expect a warrant to search filing cabinets for evidence of drug activity to prospectively restrict the search to 'file cabinets in the basement' or to file folders labeled 'Meth Lab' or 'Customers.' And there is no reason to so limit computer searches." 659 F.3d 527, 538 (6th Cir. 2011); *see also United States v. Conrad*, No. 3:12-cr-134-J-34TEM, 2013 WL 4028273, at *8

(M.D. Fla. Aug. 7, 2013) (quoting *Richards*, 659 F.3d at 539, and explaining "[f]ederal courts applying a reasonableness analysis on a case-by-case basis 'have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers'"). But additionally, defendant ignores that the application for the warrant specifically requested authorization to search for violations of Section 1030, and the warrant itself repeatedly referenced seizure from defendant's computers of evidence "as it relates to the crime under investigation." Where a warrant is "already adequately particularized based on the subject matter limitation to evidence related to [a particular crime], . . . an additional temporal limitation was not required." *United States v. Harvey*, CRIMINAL ACTION NO. 1:15-cr-00053-TWT-RGV-1, 2015 WL 9685908, at *14 (N.D. Ga. Nov. 30, 2015) (report and recommendation adopted by *United States v. Harvey*, 2016 WL 109984 (N.D. Ga. Jan. 8, 2016)) (citing *United States v. Lee*, Criminal Action File No. 1:14-cr-227-TCB-2, 2015 WL 5667102, at *10 (N.D. Ga. Sept. 25, 2015)); *see also Lee*, 2015 WL 5667201, at *10 (warrants did not need to be temporally restricted where they "were already adequately particularized based on the subject matter limitation"). The warrant was particularized based on its subject matter, no temporal limitation was required, and in any event, the extreme limitation suggested by defendant is unreasonable.

Defendant also ignores that SA Norris's affidavit established probable cause to believe that a computer within defendant's residence had been used to conduct the

intrusions. Accordingly, Attachment A specified that the place to be searched was defendant's residence, and Attachment B provided that all computers within that residence could be seized and then searched for specific items that constitute evidence of the crimes under investigation. Doc. 132-4. Defendant generically claims that the residential search warrant was overbroad, although he does not even attempt identify any item in "Attachment B" that would not have been of evidentiary value. *Cf. Lee*, 2015 WL 5667102 at *9 ("The fact that [a] warrant call[s] for seizure of a broad array of items does not, in and of itself, prove that the warrant fails to meet this requirement of particularity." (quoting *United States v. Sugar*, 606 F. Supp. 1134, 1151 (S.D.N.Y. 1985))). Defendant also claims that the warrant "allowed for the unrestricted seizure of all forms of electronic systems and data without regard to the type of information sought and without any limitation on the timeframe relevant to the charge under investigation." Doc. 132 at 19. This is false. Attachment B paragraph 1 plainly allows for the seizure of "[c]omputers and electronic storage media" and then authorizes the search of those items and seizure of an enumerated list of items of evidentiary value, listed in paragraph 4 of Attachment B. Doc. 132-4 at 2. Each of the evidentiary items listed paragraph 4 of Attachment B has readily apparent evidentiary value in this case.[3] The warrant was appropriately tailored to the facts of this case.

[3] Item 4(a) allowed for the search of "evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted . . . ." In other words, item 4(a) allowed for the seizure of attribution evidence that would identify who was using a device at the time the crime was committed. Attribution evidence may be specific to a particular

IV. The search did not exceed the scope of the warrant

Defendant next reviews case law regarding plain view computer searches but does not connect this law to his case. To the extent defendant intends to complain that agents encountered child sex abuse material on some of his computers – which now forms the basis of several charges against him – defendant ignores that upon

---

date and time, or may be broader to the extent that it identifies the person who was the regular or exclusive owner or user of a computer. Likewise, items 4(e) and 4(i) constitute attribution evidence.

Item 4(b) allows for seizure of computer software, including software used for remote access. The existence of remote access software on defendant's computers plainly was of evidentiary value in the investigation. The existence of pertinent software on a device during the setup for the intrusions, during the intrusions themselves, or at the time the device was seized is of evidentiary value.

Item 4(c) relates to the presence of malicious software that could allow others to control a computer. This is relevant to eliminate the possibility that some other actor remotely used defendant's computer to commit the intrusions. The same logic applies to item 4(d) (evidence of the absence of malicious software).

Item 4(f) seeks evidence of the computer user's "state of mind as it relates to the crime under investigation." Again, this evidence is limited to state of mind *as it relates to the crime under investigation*, and is therefore appropriately subject matter and time-limited. Plainly, the perpetrator's state of mind, intent, and motive are of evidentiary value.

Item 4(g) relates to the attachment to a computer of other storage devices. This has evidentiary value because it may provide investigative leads showing where additional evidence may be stored.

Item 4(h) relates to counterforensic programs designed to eliminate data from a computer. The presence of such programs would be indicative of consciousness of guilt and therefore constitute evidence.

Item 4(j) allows the seizure of passwords and the like, which are necessary to fully execute the warrant. Likewise, item 4(k) allows for seizure of documentation and manuals necessary to execute the warrant. Item 4(n) allowed for seizure of contextual information to understand the evidence described in other items of Attachment B.

Item 4(l) allows for seizure of information about Internet Protocol (IP) addresses used by a computer. As described in the affidavit, the defendant's IP address was pertinent to establishing probable cause for the warrant and is therefore of evidentiary value. Likewise, 4(m) allowed for seizure of records regarding the computer user's internet activity. Given that defendant used multiple websites and the internet to complete the setup for the crime and the intrusions, this was obviously of evidentiary value.

discovering child sex abuse material on his iPhone 7, agents immediately discontinued their search and sought a stand-alone warrant to search the device for child sex abuse material. *See* Case No. 3:19-mj-1284-JBT (search warrant dated August 2, 2019, authorizing search of defendant's iPhone 7 for evidence of receipt and possession of child pornography). Agents then discovered child sex abuse material on a hard drive, which is a separate device seized from defendant's residence, and again immediately discontinued their search and sought a stand-alone warrant to search that device for child sex abuse material. *See* Case No. 3:19-mj-1375-JBT (search warrant dated October 19, 2019, authorizing the search of an ACOM hard drive for evidence of receipt and possession of child pornography). Agents also found child sex abuse material on the computer seized by consent from defendant's storage locker. Ultimately, the FBI obtained search warrants to search each and every computer seized from defendant's residence for evidence of receipt or possession of child sex abuse material. *See* Case Nos. 3:19-mj-1367-JBT through 3:19-mj-1385-JBT.

In any event, agents were authorized to review photos and videos and other indicia of ownership and control of the computers because that evidence (attribution evidence) was essential to determining who was controlling the computer(s) used to commit the network intrusion they were investigating. *See* Doc. 132-4 ¶ 4(a). Attribution evidence can reasonably date from any time and may be indicative of whether a person was the sole or joint user of a device, and if the device was jointly

used, who was using it on a particular date and time. Once agents inadvertently discovered child sex abuse material on the iPhone 7 and the ACOM hard drive, they immediately ceased their review and sought warrants to review the devices for that evidence. This fact alone demonstrates that the agents were conducting a reasonable review for evidence of violations of Section 1030.

Defendant also complains that "even a valid search warrant does not give police permission to search persons present at the site of the search," citing *Ybarra v. Illinois*, 444 U.S. 85 (1979). Doc. 132 at 20. Defendant then complains that his "unlocked cell phone [was taken] from his hand while he was talking to his wife" – in other words, he acknowledges that the phone was in plain view in his hand while he was inside the residence at the time the warrant was executed. *Id.* The phone was a "computer" that agents were authorized to seize pursuant to the warrant. *See* Doc. 132-4 at 3, 5 (defining "computer" to include, among other things, "mobile phones" and authorizing the seizure of "computers"). Defendant's phone was *not* seized as a result of a search of his person. Agents did not have to pat him down to find it. Defendant's proposed interpretation of the law would mean that officers executing a residential search warrant for drugs could not seize a kilogram of cocaine if it were in the defendant's hands. That plainly is not the law, and it is not reasonable. There is no basis to suppress the seizure of the phone.[4]

[4] In any event, defendant misconstrues *Ybarra*, which in fact supports that defendant's person could be searched. In *Ybarra*, the court suppressed the search of the person of a patron of a tavern who was not the subject of the investigation but happened to be present when a warrant to search the

V. Agents executed the search warrant in a reasonable manner

Defendant next argues that his Fourth Amendment rights were violated because agents did not "knock and announce," did not immediately allow him to see the warrant, and because they excluded him from his home while executing the warrant. According to defendant's own recitation of the facts, agents knocked on defendant's door, and defendant's child answered. Doc. 132 at 4. Defendant then "joined the entry team" and was informed that the agents were there to execute a warrant. *Id.* The agents "demanded" that defendant "call his wife to have the couple's son removed from the home before they would share any information with him." *Id.*

A. Agents did not violate the "knock and announce" rule

Federal law provides that agents executing a warrant may make *forcible* entry to a home after providing notice of their "authority and purpose" and if they are refused admittance. 18 U.S.C. § 3109. There is nothing in this law that requires agents to yell through the door who they are and their purpose, rather than patiently waiting for the door to be answered and calmly explaining their authority and purpose prior to making entry, as they did here. There was no violation of the

---

tavern was executed. 444 U.S at 88-89. Ybarra was charged with possessing heroin based on that search and moved to suppress the search warrant as to himself. The Supreme Court reasoned that "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person." *Id.* at 91. The Supreme Court also found that there *was* probable cause to search the bartender, who was the subject of the investigation. *Id.* at 92. Defendant is not like Ybarra – he is like the bartender. He was the subject of this investigation, and a search of his person for his cell phone (something ordinarily stored on one's person) while he was inside the residence would have been reasonable.

knock and announce rule, and in fact, the agents' restraint in making entry to defendant's home was designed to avoid traumatizing his young child.

B. Agents provided a copy of the warrant, and even if they had not, this is not a basis to suppress the evidence in this case

Defendant submits that he "asked to see the warrant" after agents entered his home and that "[i]t was unreasonable to refuse to show the warrant and to demand that he call his wife to have their son removed from the home." Doc. 132 at 20. Defendant states that he was provided with a copy of the warrant, although he does not specify when this occurred. *Id.* at 5. Defendant claims that he was not provided with Attachments A and B, and "was told he was not allowed to view them." *Id.*

Rule 41(f)(1)(C) requires that "[t]he officer executing the [search] warrant must give a copy of the warrant and a receipt for the property taken to the person from whom" the property was taken. In *United States v. Grubbs*, 547 U.S. 90 (2006), the Supreme Court held that "[i]n fact . . . neither the Fourth Amendment nor [Rule 41] imposes such a requirement" that "the executing officer must present the property owner with a copy of the warrant before conducting his search." 547 U.S. at 98-99; *see also United States v. Neth*, No. 6:09-cr-210-Orl-19GJK, 2010 WL 1257695, at *10 (M.D. Fla. Mar. 30, 2010) ("[T]he Fourth Amendment does not require an executing officer to present a property owner with a copy of the warrant before conducting or during his search of the premises." (citing *Grubbs*, 547 U.S. at 98-99)). The Supreme Court further stated that "[t]he absence of a constitutional requirement

that the warrant be exhibited at the outset of the search, or indeed until the search has ended is . . . evidence that the requirement of particular description does not protect an interest in monitoring searches." 547 U.S. at 99. Furthermore, "[t]he Constitution protects property owners not by giving them license to engage the police in a debate over the basis for the warrant," but rather beforehand by requiring review of the warrant by a judicial officer and afterward by providing "a right to suppress evidence improperly obtained and a cause of action for damages."[5] *Id.*

If this Court were to conduct a hearing on this issue, the United States expects it would present testimony from agents that defendant did not repeatedly request to see the warrant as he now claims, and furthermore that a copy of the warrant and its attachments were left in defendant's residence. In any event, a hearing on this issue would be a waste of judicial resources because even if defendant's version of events were credited, there would be no basis to suppress the warrant.

C. Agents were entitled to exclude defendant from his home while executing the warrant

Defendant contends that the FBI had no authority to remove him from his home while they executed the search warrant. Doc. 132 at 21. Defendant is wrong. *United States v. Correa*, 347 F. App'x 541, 545 (11th Cir. 2009) ("Because the

[5] Defendant cites *United States v. Wuagneux*, 683 F.2d 1343, 1348 (11th Cir. 1982) for the contention that a "warrant is still valid so long as the document containing the description [of the items to be seized] is attached to the warrant and accompanies it at the time of execution." Doc. 132 at 22. The undersigned could not locate this particular holding in *Wuagneux*. The *Wuagneux* Court did note that it was "preferable" that the person whose premises are searched "be informed of the searching agents' authority at the time of the search," but because the appellant had access to the warrant materials when litigating his motion to suppress, there was no constitutional error.

occupants were aware of the investigation, the agents were entitled to secure the houses to prevent the destruction of evidence." (citing *United States v. Tobin*, 923 F.2d 1506, 1512 (11th Cir. 1991))). In fact, the FBI could have lawfully detained defendant during the search. *See Michigan v. Summers*, 452 U.S. 692, 701-02 (1981) (holding that police are entitled to detain a resident while his home is searched, pursuant to a warrant, for contraband); *Croom v. Balkwill*, 645 F.3d 1240, 1250-51 (11th Cir. 2011) (stating that a "fair reading" of *Summers* "implies that law enforcement officers are entitled to detain occupants of a premises for the whole length of most warranted searches"). The FBI was entitled to secure the home during the search, and defendant has submitted no authority that would support his position that he should have been free to roam the premises during the search.

CONCLUSION

Defendant has not set forth a sufficient basis to warrant a *Franks* evidentiary hearing and none should be granted. Additionally, defendant has also not demonstrated that the search warrant lacked probable cause, that it was overbroad, that it was insufficiently particular, that its scope was exceeded upon execution, or any flaw in its execution. Defendant's motion to suppress should be denied.

Respectfully submitted,

ROGER B. HANDBERG
United States Attorney

By: */s/ Laura Cofer Taylor*
LAURA COFER TAYLOR
Assistant United States Attorney

USAO No. 170
300 N. Hogan Street, Suite 700
Jacksonville, Florida 32202
Telephone: (904) 301-6300
Facsimile: (904) 301-6310
E-mail: laura.c.taylor@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on November 15, 2022, I electronically filed the foregoing with the Clerk of the Court by using the CM/ECF system which will send a notice of electronic filing to the following:

Christopher Eric Roper, Esq.
Standby Counsel for Defendant

I hereby certify that on November 15, 2022, a true and correct copy of the foregoing document and the notice of electronic filing were placed in the United States Mail addressed to the following non-CM/ECF participant(s):

Samuel Arthur Thompson, pro se
Baker County Detention Center
P.O. Box 1629
MacClenny, FL 32063

s/ Laura Cofer Taylor
LAURA COFER TAYLOR
Assistant United States Attorney