IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA,

v.

VIKAS SINGLA,

Defendant.

CRIMINAL ACTION NO.
1:21-CR-00228-MLB-RDC

NON-FINAL REPORT AND RECOMMENDATON

Pending before this Court is Defendant Vikas Singla's Motion to Dismiss Indictment for lack of specificity or for a Bill of Particulars, [Doc. 29]. The Government filed its brief opposing this motion on June 30, 2022, [Doc. 38]. Mr. Singla filed his reply brief on September 1, 2022, [Doc. 45]. Following careful review of the parties' pleadings, counsels' oral arguments (R. 50), and the applicable law, this motion is ripe for review. For the reasons stated below, the

undersigned **RECOMMENDS** that Defendant's Motion to Dismiss Indictment be **GRANTED** and that his request for a Bill of Particulars be **DENIED AS MOOT**. [1]

I. BACKGROUND

Mr. Singla is charged in an eighteen-count Indictment with offenses involving violations of the Computer Fraud and Abuse Act of 1986 ("CFAA"). [Doc. 1]. Count One states:

> On or about September 27, 2018, in the Northern District of Georgia and elsewhere, the defendant, VIKAS SINGLA, aided and abetted by others unknown to the Grand Jury, knowingly caused and attempted to cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused and attempted to cause damage without authorization to a protected computer — that is, one or more computers used by Gwinnett Medical Center that operated the Duluth, Georgia hospital's Ascom phone system — and the offense caused and would, if completed, have caused: a. loss to Gwinnett Medical Center during the one-year period from SINGLA's course of conduct affecting protected computers aggregating at least $5,000 in value; b. the modification, impairment, and potential modification and impairment of the medical examination, diagnosis, treatment and care of one or more individuals; and c. damage affecting at least 10 protected computers during a one-year period in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b) and (c)(A)(B) and Section 2.

[Doc. 1 at 2].

[1] Also pending before this Court are the following motions: Motion for Issuance of Rule 17(c) Subpoenas [Doc. 26], Motion to Dismiss Indictment for failure to state an offense [Doc. 27], Motion to Dismiss Count 18 of the Indictment as unconstitutionally vague [Doc. 28] and Motion to Compel disclosure of grand jury transcripts [Doc. 30]. Based on this Court's recommendation regarding the instant Motion to Dismiss Indictment, all of these motions are **DENIED AS MOOT**. However, if the District Judge declines to adopt this Report and Recommendation, Mr. Singla is directed to renew these motions within 21 days of the filing of the District Judge's Order.

Counts Two through Seventeen (which include a Table identifying sixteen printers as "protected computers") allege the following:

On or about September 27, 2018, in the Northern District of Georgia and elsewhere, as specified in the following table, the defendant, VIKAS SINGLA, aided and abetted by others unknown to the Grand Jury, knowingly caused and attempted to cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused and attempted to cause damage without authorization to a protected computer — that is, one or more computers used by Gwinnett Medical Center in the Duluth and Lawrenceville, Georgia hospitals that operated the printers identified in the following table — and the offense caused and would, if completed, have caused: a. loss to Gwinnett Medical Center during the one-year period from SINGLA's course of conduct affecting protected computers aggregating at least $5,000 in value; and b. the modification, impairment, and potential modification and impairment of the medical examination, diagnosis, treatment and care of one or more individuals…in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and (c)(4)(B) and Section 2.

[Doc. 1 at 3-4].

Count Eighteen alleges:

On or about September 27, 2018, in the Northern District of Georgia and elsewhere, the defendant, VIKAS SINGLA, aided and abetted by others unknown to the Grand Jury, intentionally accessed and attempted to access a computer without authorization and exceeded and attempted to exceed authorized access to a computer, and thereby obtained and attempted to obtain information from a protected computer, that is, a Hologic R2 Digitizer used by Gwinnett Medical Center in the Lawrenceville, Georgia hospital, and the offense was committed for purposes of commercial advantage and private financial gain, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (b), (c)(2)(B)(i), and Section 2.

[*Id.* at 5].

All of these Counts incorporate by reference the introduction that states Gwinnett Medical Center ("GMC") was a not-for-profit health care network that

provided health care services for two hospitals located in the Northern District of Georgia. [Doc. 1 at 1]. Mr. Singla was the chief operating officer of a network security company that provided services to the health care industry. [*Id.*]. According to the Government, Mr. Singla committed a cyberattack against GMC's Lawrenceville and Duluth hospitals between September 27, 2018 and October 2, 2018. [Doc. 26 at 1]. This attack temporarily interrupted GMC's internal telecommunications system causing GMC's printers to begin printing several sheets of paper. [*Id.*] As a result, Mr. Singla obtained the names and dates of birth of GMC patients. [*Id.*]. After GMC publicly denied it had been the victim of a cybersecurity breach, an unknown person posted the names of some of the patients and their dates of birth on the social networking service *Twitter* in order to contradict GMC's denial. [*Id.* at 1-2]. The Government believes Mr. Singla was the person responsible for posting this confidential information. [*Id*. at 2].

As agents with the Federal Bureau of Investigation began conducting their investigation into this incident (beginning as early as September 27, 2018), GMC retained the services of the King and Spalding, LLP law firm and a consulting firm – PricewaterhouseCoopers, LLP – to assist in its breach remediation efforts. [Doc. 26 at 2]. On June 8, 2021, a grand jury returned the pending Indictment against Mr. Singla alleging the above listed offenses. [Doc. 1].

II. THE PARTIES' CONTENTIONS

Mr. Singla submits that the Indictment must be dismissed because it lacks the specificity required by the Sixth Amendment to the Constitution and Federal Rules of Criminal Procedure 12(b)(3)(B)(iii) and 7(c)(1)[2]. The alleged deficiencies include the absence of essential facts "necessary for [him] to prepare his defense, avoid prejudicial surprise, or plead double jeopardy." [Doc. 29 at 3]. The essential facts he claims are missing in the first seventeen counts include the nature of the "transmission" that occurred, the "program, information, code or command" he allegedly transmitted, the "damage" his conduct caused to the "protected computers," whether all of the computers mentioned throughout the Indictment were the "protected computers" that were compromised, what "loss" GMC allegedly sustained and how his conduct "modifi[ed]" "impair[ed], or "potential[ly] modif[ied] or impair[ed]…the medical examination, diagnosis, treatment or care of

[2] Rule 12(b)(3)(B)(iii) of the Federal Rules of Criminal Procedure allows a defendant to raise a pretrial motion alleging "a defect in the indictment or information including…lack of specificity." Fed. R. Crim. P. 7 (c)(1) states that: "[t]he indictment or information must be a plain, concise, and definite statement of the essential facts constituting the offense charged and must be signed by the attorney for the government. It need not contain a formal introduction or conclusion. A count may incorporate by reference an allegation made in another count. A count may allege that the means by which the defendant committed the offense are unknown or that the defendant committed it by one or more specified means. For each count, the indictment or information must give the official or customary citation for the statute, rule, regulation, or other provision of law that the defendant is alleged to have violated."

one or more individuals." [Doc. 29 at 10-11]. These factual omissions are particularly problematic, he argues, given the highly technical nature of the elements of the charged offenses. [*Id*].

As for Count Eighteen, Mr. Singla avers that the Indictment is insufficient because it fails to explain how he allegedly "exceeded" or "attempted to exceed authorized access" to a computer, whether he was notified by GMC of the limitations of his access, to what degree his access was "without authorization," which computer he allegedly accessed without the requisite authorization and how the device described in this Count qualifies as a "protected computer" as defined by the CFAA. [Doc. 29 at 11-12]. Based on these myriad omissions, Mr. Singla argues that the Indictment is constitutionally infirm and due to be dismissed.[3]

The Government argues Mr. Singla's claims are meritless because the Indictment provides the factual specificity required by Fed. R. Crim. P. 7 (c)(1) and Circuit precedent. [Doc. 38 at 2-3]. It asserts that Mr. Singla "does not lack the information necessary for him to understand the charges filed against him and prepare his defense," noting that his detailed pretrial motions undermine his argument that he is unaware of the nature of the criminal allegations or would suffer

[3] Mr. Singla also requested production of a Bill of Particulars based on these same alleged factual omissions. [Doc. 29 at 14]. Because this Court recommends that the Indictment be dismissed because it lacks specificity, the request for a Bill of Particulars is **DENIED AS MOOT** and will not be addressed herein.

"prejudicial surprise" if required to defend himself against the Indictment in its present form. [Doc. 38 at 7]. The Government also argues that Mr. Singla's claimed inability to raise a double jeopardy claim is specious because the Indictment includes descriptions of the "protected computers," their locations, and the dates he allegedly attacked them "in each count of the indictment." [*Id*. at 9]. Moreover, in reference to the "protected computers" listed in Counts Two through Seventeen, the Government emphasizes that the Indictment specifically identifies them as "computers used by Gwinnett Medical Center in Duluth and Lawrenceville, Georgia hospitals that operated the printers [listed in the Table] by their make, model, device identifier, and their assigned IP address." [*Id.*]. The fact that the Indictment tracks the language of the statutes, provides dates of the alleged events and "identifies numerous specific factual details," the Government continues, it is sufficiently specific. [*Id.* at 4].

Lastly, the Government avers that the "essential facts" Mr. Singla claims are missing have either already been produced in accordance with Fed. R. Crim. Proc. 16 (a)(1) (Rule governing Discovery and Inspection) or consist of "legal questions that do not need to be briefed in the indictment." [Doc. 38 at 5]. Because the Government believes Mr. Singla is merely seeking disclosure of evidence pertaining to its trial strategy - as opposed to facts needed to adequately inform him of the

charges against him - it submits dismissal of the Indictment and disclosure of the requested evidence are unwarranted.

In response, Mr. Singla reiterates his assertion that the Indictment is woefully deficient; lacking specificity regarding the illegal conduct he allegedly engaged in and clarity regarding the specific computers that are the subject of the prosecution. [Doc. 45 at 1-2; 6]. Furthermore, he asserts that because the Indictment fails to clearly specify which computers are considered the "protected computers," this uncertainty could create multiplicity problems – "if [GMC's] print servers are the 'protected computers' at issue in each count, rather than the printers themselves, then the government has likely improperly charged [him] with multiple crimes for the same conduct." [*Id.* at 7]. Mr. Singla avers that this ambiguity, coupled with the alleged factual omissions, compels dismissal of the Indictment in its entirety.

III. LEGAL STANTARDS

The Fifth Amendment provides that "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury." U.S. Const. amend. V. The Sixth Amendment guarantees that "In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed…and to be informed of the nature and cause of the accusation." U.S.

Const. amend. VI. These rights, as well as the Due Process Clause of the Fifth Amendment, are brought to bear when a defendant challenges the sufficiency of an indictment." See, *Russell v. United States,* 369 U.S. 749, 761 (1962).

Pursuant to Fed. R. Crim Proc. 12 (b)(3)(B)(iii), a defendant may file a motion to dismiss an indictment for failure to provide sufficient specificity. In ruling on this motion, this Court is limited to reviewing the face of the indictment. *United States v. Salman,*378 F.3d 1266, 1268 (11th Cir. 1999). It is well-established that "[t]here is no summary judgment procedure in criminal cases. Nor do the rules provide for a pre-trial determination of sufficiency of the evidence." *United States v. Critzer,* 951 F.2d 306, 307 (11th Cir.1992)). "It is generally sufficient that an indictment set forth the offense in the words of the statute itself, as long as 'those words of themselves fully, directly, and expressly, *without any uncertainty or ambiguity*, set forth all the elements necessary to constitute the offence intended to be punished.' " *Hamling v. United States,* 418 U.S. 87, 117(1974) (citing, *United States v. Carll,* 105 U.S. 611, 612 (1882))(emphasis added). Merely reciting the elements of the applicable statutes is not sufficient if the indictment fails to put the Defendant on fair notice of the charges he faces: " 'Undoubtedly the language of the statute may be used in the general description of an offence, but it must be accompanied with such a statement of the facts and circumstances as will inform the accused of the specific offence,

coming under the general description, with which he is charged.' " *Hamling* at 117–18 (quoting, *United States v. Hess,* 124 U.S. 483, 487 (1888)).

The Supreme Court adopted the following test to determine whether an indictment is sufficient:

> [A]n indictment is sufficient if it, first, contains the elements of the offense charged and fairly informs a defendant of the charge against which he must defend, and, second, enables him to plead an acquittal or conviction in bar of future prosecutions for the same offense.

Hamling, 418 U.S. 87, 117 (1974)(citing, *Hagner v. United States,* 285 U.S. 427, (1932)).

Consequently, an indictment that fails to apprise the defendant "with reasonable certainty, of the nature of the accusation against him is defective,…although it may follow the language of the statute." *United States v. Simmons*, 96 US. 360, 362 (1877); See also, *United States v. Sumner*, 89 F. Supp. 3d 1161, 1166 (N.D. Okla. 2015)(where district court granted motion to dismiss indictment charging the defendant with failure to register under the Sex Offender Registration and Notification Act (SORNA) because it did not put him on fair notice of the crime alleged, leaving "the Court to guess the factual basis for the indictment returned by the grand jury.").

In *Russell, supra,* the Supreme Court held that the indictment in that case was insufficient because it "failed to sufficiently apprise the defendant 'of what he

must be prepared to meet.'" *Russell*, 369 U.S. at 764. The defendants in *Russell* had been charged with refusing to answer questions when summoned before the House Committee on Un–American Activities and a Senate subcommittee. *Russell*, 369 U.S. at 752-3. Although the indictment set out the date and each question the defendants refused to answer, it only generically alleged that the questions were pertinent to the subject that was the basis of the congressional inquiry. *Id.* The Court found that these generic allegations did not provide sufficient notice to the defendants, holding: "[W]here the definition of the offence ... includes generic terms, it is not sufficient that the indictment shall charge the offence in the same generic terms as in the definition; but it must state the species,—it must descend to particulars." *Id.* at 765 (citing, *United States v. Cruikshank,* 92 U.S. 542, 558 (1875)). The vague description of the nature of the inquiry "left the prosecution free to roam at large—to shift its theory of criminality so as to take advantage of each passing vicissitude of the trial and appeal." *Russell*, 369 U.S. at 768.

The *Russell* Court also found that the indictment deprived the defendants of their right to be charged by a grand jury: "To allow the prosecutor, or the court, to make a subsequent guess as to what was in the minds of the grand jury at the time they returned the indictment would deprive the defendant of a basic protection which the guaranty of the intervention of a grand jury was designed to secure. For a

defendant could then be convicted on the basis of facts not found by, and perhaps not even presented to, the grand jury which indicted him." *Russell,* 369 U.S. at 770. Notably, the Court concluded that those deficiencies could not be cured by a bill of particulars. *Id.*; See also, *United States v. Peterson*, 544 F. Supp. 2d 1363, 1375 (M.D. Ga. 2008)(explaining that a bill of particulars could not cure an indictment that failed to specify what acts the defendant allegedly committed without running afoul of the Fifth Amendment.).

IV. DISCUSSION

As noted above, the Government argues that the Motion to Dismiss should be denied because the essential facts and elements of the charged offenses are contained in the Indictment. It also asserts that Mr. Singla's demands for specifics regarding how he allegedly committed the offenses should be rejected because this evidence has already been provided. [Doc. 38 at 1, 7-8]. As for Mr. Singla's requests for specification regarding which computers it deems are "protected computers" and how his access to these computers was "unauthorized," the Government claims these constitute questions of law not subject to disclosure. [*Id.* at 5]. The Government also submits that these latter requests are attempts to compel disclosure of its trial strategy, disclosures not required by Supreme Court or Circuit precedent.[*Id.*]. This Court disagrees.

First of all, although the Indictment sets out the elements of each charged offense, it must also "be accompanied with such a statement of facts and circumstances as will inform the accused of the specific offence, coming under the general description, with which he is charged." *Hamling*, 418 U.S. at 117-18 (quoting *Hess*, 124 U.S. at 483). As noted by Mr. Singla, the Indictment does not reveal how he allegedly transmitted computer code resulting in financial loss to GMC, how the transmission resulted in the "modification, impairment, and potential modification and impairment of the medical examination, diagnosis, treatment and care of one or more individuals" or how the transmission damaged at least 10 "protected computers." Even if an indictment follows the language of the applicable statutes, it is defective if it is "not framed to apprise the defendant, with reasonable certainly, of the nature of the accusations against him." *United States v. Bobo*, 344 F.3d 1076, 1083 (11th Cir. 2003).

Furthermore, the Government's argument that Mr. Singla's requests constitute legal questions that need not be explained in the Indictment demonstrates a misunderstanding of due process considerations and the procedural posture of this case. Mr. Singla cannot craft a legal challenge to these charges unless the Indictment clearly articulates *which* computers are the "protected computers" and *what* specific conduct involved transactions made via "unauthorized access." These

are *questions of fact* the Indictment should contain to allow Mr. Singla to raise *issues of law* at the appropriate time.

An analogous scenario from this District is instructive in this context. In *United States v. Tripodis*, No. 1:18-cr-240-1-TWT-JFK, 2020 WL 914681 (N.D. Ga., Feb. 26, 2020), the defendant was charged in a multi-count indictment with offenses involving wire fraud and mail fraud. He moved to dismiss the indictment alleging that it was insufficient because it did not include every element of each offense. *Id.* at. *1. Specifically, he argued that the failure to identify the victims of the fraud scheme and the property interests that were defrauded rendered the indictment insufficient. *Id*. The government argued it was not required to identify the victims of the fraud. *Id.* It also submitted that dismissal was unwarranted because six possible classes of victims and the property interests affected by the defendant's scheme were revealed in its supplemental brief and in a previous indictment returned against the defendant in a related case. *Id.* at *1-2.

The Magistrate Judge agreed with the government, finding that the information sought by the defendant was incorporated by reference in the "background" and "manner and means" paragraphs of the indictment. *Tripodis* at *1. She concluded that the essential elements of the offenses were sufficiently pleaded, and that the facts contained in the supplemental brief and prior indictment adequately advised

defendant of the nature of the fraud scheme alleged in the pending indictment. *Tripodis*. at *3. The court also found defendant's complaint that failure to specifically identity the victims might prevent jury unanimity could be addressed at trial. *Id.* at *1.

The defendant filed objections to the report and recommendation, reasserting his claim that the indictment's failure to specify *who* was victimized and *what* property was compromised rendered the indictment insufficient. *Tripodis*, at *1-2. The District Judge agreed. He found that the Magistrate Judge's conclusion that the scheme to defraud was clearly set forth in the "background" and "manner and means" portions of the conspiracy charge "misse[d] the point that nothing in the indictment identifies who is being defrauded of what." *Id.* at *3. The Court acknowledged that the mail fraud and wire fraud statutes require the government to prove that the defendant "intended to defraud *someone*," and that a "scheme to defraud" means a plan or course of action intended to "deceive or *cheat someone out of money or property* using false or fraudulent pretenses, representations, or promises." *Id.* (emphasis in original). Because "the indictment in this case [did] not allege who the 'someone' is or what 'money or property' they are to be cheated out of," the Court concluded that the indictment failed to apprise the defendant "with reasonable certainty of the nature of the accusation against him." *Tripodis* at *3. As

a result, the District Judge declined to adopt the report and recommendation and granted defendant's motion to dismiss.

Likewise, in the case at bar, the Indictment fails to apprise Mr. Singla "with reasonable certainty of the nature of the accusation[s]." The CFAA defines "protected computer" to mean a computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information" (18 U.S.C. § 1030(e)(8)), and "loss" means "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 interruptions of service." 18 U.S.C. § 1030(e)(11). With respect to Count Eighteen, "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

The pattern jury instructions applicable to the charged offenses are as follows. Count One: (1) defendant knowingly caused or attempted to cause the transmission of a program, information, code, or command, (2) as a result of such conduct, the

defendant intentionally caused or attempted to cause damage without authorization, (3) the damage was to a protected computer, and (4) the offense caused (a) loss affecting protected computers aggregating at least $5,000 in value during a one-year period, (b) the modification, impairment, or potential modification or impairment of the medical examination, diagnosis, treatment or care of one or more individuals, or (c) damage affecting at least 10 protected computers during a one-year period. Eleventh Circuit Pattern Jury Instructions (Criminal Cases) 2022, No. O42.3 (as modified).

In order to obtain convictions on Counts Two – Seventeen, the Government must prove beyond a reasonable doubt that: (1) defendant knowingly caused or attempted to cause the transmission of a program, information, code, or command, (2) as a result of such conduct, the defendant intentionally caused or attempted to cause damage without authorization, (3) the damage was to a protected computer, and (4) the offense caused (a) loss affecting protected computers aggregating at least $5,000 in value during a one-year period, or (b) the modification, impairment, or potential modification or impairment of the medical examination, diagnosis, treatment or care of one or more individuals. Eleventh Circuit Pattern Jury Instructions (Criminal Cases) 2022, No. O42.3 (as modified).

As for Count Eighteen, the elements of this offense include the following: (1) that defendant intentionally accessed a computer without authorization or exceeded his authorized access to a computer, (2) by accessing the computer the defendant obtained information from a protected computer, and (3) the offense was committed for commercial advantage or private financial gain. Eleventh Circuit Pattern Jury Instructions (Criminal Cases) 2022, No. O42.2 (as modified).

Given the CFAA's distinctive technical definitions, the Indictment must reveal which computers are considered the "protected computers" that were unlawfully accessed resulting in "damage" to GMC and other individuals to allow Mr. Singla to prepare his defense and ensure he does not face a subsequent prosecution based on the same conduct. He must also be informed of the degree of access he maintained and how he allegedly exceeded the scope of that authorization. For instance, the introduction states that Mr. Singla is the chief operating officer of a network security company that provides services for the healthcare industry. [Doc. 1]. The Indictment does not reveal what professional relationship he had (if any) to GMC, to what extent he had access to GMC's internal network or to what degree he exceeded his authority while accessing GMC's computer system. cf., *United States v. Hutchins*, 361 F. Supp. 3d 779, 793 (E.D. Wisc., Feb. 11, 2019)(where defendant's motion to dismiss indictment charging him

with violating the CFAA was denied after the court found the indictment specifically advised him of the nature of the charges. Each element of the offenses was listed along with the nature of the offenses, "including the software at issue," how defendant developed the malware that damaged the computers, and how he marketed the malware to specific customers.).

Mr. Singla's concern is well founded given the Supreme Court's recent decision in *Van Buren v. United States*, 141 S.Ct. 1648 (2021), where the Court resolved a decades-long circuit split concerning whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the CFAA if she accesses the same information for an improper purpose. In vacating Mr. Van Buren's conviction, the High Court rejected the government's contention that the statute covers a broad range of improper computer access including circumstances in which an individual accessed a computer with an improper purpose, holding that the "exceeds authorized access" prohibition only "covers those who obtain information from particular areas in the computer – such as files, folders or databases – to which their computer access does not extend. It does not cover those who, like Van Buren, have improper motives for obtaining information that is otherwise available to them." *Id*. at 1662. This ruling significantly narrowed the scope of liability under the statute, clarifying that the

CFAA is primarily directed toward hackers who access or obtain information they do have permission to access. *Van Buren*, 141 S. Ct. at 1661-62. Thus, clarification of the conduct the Government contends violated the CFAA in the instance case is imperative if Mr. Singla is to be properly apprised on the nature of the alleged violations. "Where guilt depends so crucially upon such a specific identification of fact, our cases have uniformly held that an indictment must do more than simply repeat the language of the criminal statute." *Russell, 369 U.S. at 764*.[4]

CONCLUSION

Based on the foregoing reasons, the undersigned **RECOMMENDS** that Mr. Singla's Motion to Dismiss Indictment [Doc. 29] be **GRANTED**. Having

[4] The Government's reliance on *United States v. Gasperini*, No. 16-cr-441-NGG, 2017 WL 2399693(E.D.N.Y. May 31, 2017) in support of its argument that the Indictment is sufficient is misplaced. In *Gasperini*, the defendant (an Italian national) argued that the indictment was insufficient because it failed to allege he accessed a "protected computer" or that he had "actual access" to computer servers in the United States; necessary elements for charges involving computer intrusion proscribed by the CFAA. *Id*. at *3-4. His motion to dismiss was denied because the indictment contained a detailed statement of facts describing his electronic transmission of malicious software in a 'click fraud' scheme that infected a network of computers without the users' knowledge or authorization. *Id.* The court emphasized that the indictment alleged "at several points that Defendant had actual access to computer servers, including access gained as part of the process of installing the malware." *Id.* at *4. It also noted that the computers were necessarily "protected computers" as defined by the CFAA because defendant was living abroad when the computers were accessed, conduct that necessarily involved internet-connected computers. *Id.* at 3. Because that indictment, unlike the one in the instant case, provided essential facts that specified the nature of the offenses the defendant allegedly committed, the opinion is factually inapposite.

not been advised of any impediments to the scheduling of a trial as to him, this case is **CERTIFIED READY FOR TRIAL.**

IT IS SO RECOMMENDED on this 28th day of November, 2022.

REGINA D. CANNON
United States Magistrate Judge