

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

**ORDER AND FINAL REPORT AND RECOMMENDATION**

Pending before this Court are five motions filed by Defendant Vikas Singla: Renewed Motion to Dismiss Indictment for Lack of Specificity, [Doc. 68], Renewed Motion to Dismiss Count Eighteen of the Indictment as Unconstitutionally Vague, [Doc. 69], Renewed Motion for a Bill of Particulars, [Doc. 71], Renewed Motion for Early Issuance of Rule 17(c) Subpoena, [Doc. 67], and Renewed Motion to Compel Disclosure of Grand Jury Transcripts, [Doc. 70]. The Government filed briefs opposing these motions on May 15, 2023, [Docs. 73, 74, 75, 76, and 77]. It also filed discovery materials under seal in support of its response to Mr. Singla's Renewed Motion for a Bill of Particulars, [Doc. 78]. Mr. Singla filed reply briefs as

to each of his renewed motions on June 16, 2023, [Docs. 83, 84, 85, 86, and 87].

These matters are now ripe for review.

## **I. FACTUAL AND PROCEDURAL 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.

[*Id.* at 2].

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 alleging the above listed offenses. [Doc. 1].

Mr. Singla filed several pretrial motions on April 20, 2022, [Docs. 26, 27, 28, 30 and 31] including a Motion to Dismiss Indictment for Lack of Specificity, or in the alternative, a Bill of Particulars. [Doc. 29]. The Government filed its responses on June 30, 2022, [Docs. 36, 37, 38, 39 and 40]. Mr. Singla filed his reply briefs on

September 1, 2022, [Docs. 44, 45, and 46]. Following review of these pleadings and oral argument by the parties on May 4, 2022, this Court issued a Report and Recommendation (“R&R”) recommending that Mr. Singla’s Motion to Dismiss Indictment for Lack of Specificity [Doc. 29] be granted and that his remaining motions be denied as moot. [Doc. 51].

The Government filed objections to this R&R on December 13, 2022, [Doc. 53]. Both parties filed supplemental briefs regarding these objections on January 13 and January 30, 2023, [Doc. 57; 58]. Following oral argument before the District Court, the Government’s objections were sustained, the R&R was rejected, and the matter remanded to the undersigned to address any pretrial motions Mr. Singla chose to renew, [Doc. 63].

Following careful review of the parties’ most recent pleadings and the applicable law, the undersigned **RECOMMENDS** that Defendant’s Renewed Motion to Dismiss Indictment for Lack of Specificity, [Doc. 68], be **GRANTED**; **RECOMMENDS** that Defendant’s Renewed Motion to Dismiss Count Eighteen of the Indictment as Unconstitutionally Vague, [Doc. 69], be **DENIED IN PART/DEFERRED IN PART**; Defendant’s Renewed Motion for Early Issuance of Rule 17(c) Subpoena, [Doc. 67], is **DENIED**; Defendant’s Renewed Motion for a

Bill of Particulars, [Doc. 71], is **DENIED**; and Defendant's Renewed Motion to Compel Disclosure of Grand Jury Transcripts, [Doc. 70], is **DENIED**.

## **II. LEGAL ANALYSIS**

### **A. Defendant's Renewed Motion to Dismiss Indictment for Lack of Specificity**

Mr. Singla asserts three claims alleging Counts One through Seventeen of the Indictment are constitutionally infirm in violation of the Due Process Clause of the Sixth Amendment, the Fifth Amendment's Grand Jury and Double Jeopardy Clauses and Fed. R. Crim. Proc. 12(b)(3)(B)(iii) and 7(c)(1). [Doc. 68]. First, he claims that Count One is unconstitutionally vague because the "protected computer" described in this count is GMC's Ascom phone system, "not a particular computer or device that bears a unique serial number or identifier." [*Id.* at 9]. According to the Government, this phone system is comprised of "hundreds of different protected computers (including at least six different servers and hundreds of handsets) any one or all of which [it] contends can be used at trial to prove the 'protected computer' element" alleged in Count One. [Doc. 68 at 7-8]. Because this phone system consists of "a collection of numerous computers and devices" as opposed to a single "protected computer" as defined by Section 1030(e)(2), Mr. Singla argues that this "vague formulation" prevents him from ensuring that the putative "protected computer" the grand jury considered when it found probable cause to bring the

underlying charge is the same one the Government will rely upon at trial to prove this offense. [Doc. 68 at 9-10]. He also argues that this ambiguity prevents him from ascertaining whether the “damage” the Government will attempt to prove at trial is the “damage” the grand jurors considered in making its probable cause determination. [*Id.*]. He claims this lack of specificity makes it “impossible to discern which, if any, particular computer [he] is under indictment for having allegedly damaged, let alone which one out of hundreds the grand jury had in mind when it approved the charges.” [*Id.* at 10-11].

Mr. Singla also claims that Counts One through Seventeen are constitutionally infirm because Section 1030(c)(3)(I) (the felony-loss provision) does not permit the Government to charge a defendant with damaging multiple “protected computers” in a single count. [Doc. 68 at 11]. He argues that the Government must allege at least one different “protected computer” other than the one that forms the basis of the underlying charge to trigger application of the enhancement. [*Id.* at 11-12]. Additionally, because the Ascom phone system consists of hundreds of “protected computers,” thereby preventing the Government from identifying a particular “protected computer,” he risks being punished twice for “damage” caused to only one “protected computer.” [Doc. 68 at 11]. This ambiguity, he continues, may result in violations of the Fifth Amendment Grand

Jury Clause and his Double Jeopardy rights because he would be “subjected to increased punishment by double-counting the same protected computer upon which the underlying charge is predicated.” [Doc. 68 at 11].

Finally, Mr. Singla submits that Counts One through Seventeen must be dismissed because they fail to allege “in common language, a particular transmission, program, code or command for which [he] is allegedly responsible, such as a particular malware, ransomware or delete command.” [Doc. 68 at 13]. He also claims that the Indictment must identify the type of “damage” that occurred to each “protected computer,” “such as disabling or overwhelming a computer server or program, or corrupting or destroying a file or data” to ensure that he is informed of the facts and circumstances of the charged offenses as required by the Sixth Amendment. [*Id.*].

The Government submits that all of these claims are meritless. [Doc. 73]. It avers that the first claim is barred from consideration because it has already been rejected by the District Court. [*Id.* at 5]. As for the remaining allegations, it claims that they are wholly unsupported by the relevant facts and applicable law. [*Id.* at 13, 18, and 21].



### Discussion

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. Fed. R. Crim. P. 7 (c)(1) provides 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.”

In ruling on a motion dismiss an indictment for failure to sufficiently apprise the defendant of the nature and circumstances of the charged offenses, this Court is limited to reviewing the face of the indictment. *United States v. Salman*, 378 F.3d 1266, 1268 (11<sup>th</sup> Cir. 1999); *United States v. Sharpe*, 438 F.3d 1257, 1236 (11<sup>th</sup> Cir. 2006). 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). However, 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)). “When the indictment used generic terms, it must state the offense with particularity.” *United States v. Bobo*, 344 F.3d 1076, 1083 (11<sup>th</sup> Cir. 2003). Hence, an indictment that fails to apprise the defendant “with reasonable certainty, of the nature of the accusation against him, to the end that he may prepare his defense, and plead the judgement as a bar to any subsequent prosecution for the same offense. An indictment not so framed is defective, although it may follow the language of the statute.” *United States v. Simmons*, 96 US. 360, 362 (1877); *United States v. Schmitz*, 634 F.3d 1247, 1261 (11<sup>th</sup> Cir. 2011)(where the court vacated defendant’s convictions upon finding the indictment was unconstitutionally vague despite the fact that it tracked the language of the statute, ruling that “the federal-funds counts allege no facts or circumstances that inform Schmitz of these specific

charges. As a result, the allegations of fraud in the federal-funds counts are insufficient as a matter of law.”).

In the instant case, Count One alleges that Mr. Singla “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.” [Doc. 1 at 2]. Counts Two through Eighteen allege that being “aided and abetted by others unknown to the Grand Jury, [he] 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”. [Doc. 1 at 3-4].

The CFAA defines the term “damage” as “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(e)(8)). “Loss” is defined as “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).

Mr. Singla’s first claim alleges that Count One is unconstitutionally vague because the “protected computer” described in this count has been identified as GMC’s Ascom phone system, “not a particular computer or device that bears a unique serial number or identifier.” [Doc. 68 at 9]. Because this system consists of “a collection of numerous computers and devices” as opposed to a single “protected computer” as defined by Section 1030(e)(2), Mr. Singla argues that it is “impossible to discern which, if any, particular computer [he] is under indictment for having allegedly damaged, let alone which one out of hundreds the grand jury had in mind when it approved the charges.” [*Id.* at 10-11]. This ambiguity, he claims, violates the Fifth Amendment Grand Jury Clause because it fails to ensure that the putative “protected computer” he allegedly damaged is the same one for which the grand jury found probable cause to support the charge. [*Id.*]. He also

avers that his Double Jeopardy rights could be infringed because he would be “subjected to increased punishment by double-counting the same protected computer upon which the underlying charge is predicated.” [*Id.* at 11].

The Government submits that Mr. Singla’s arguments are foreclosed because they consist of the same alleged errors the District Court rejected in its February 28, 2023 Order. [Doc. 73 at 6].<sup>1</sup> It claims that Mr. Singla “previously argued that “[d]escribing an unidentified group of computers (or perhaps only one—the [i]ndictment does not specify) fails to allege the ‘protected computer’ element of each offense with sufficient particularity to satisfy Rule 7(c)(1) and the Constitution.” (Doc. 45 at 4–5.) Now he argues: “Given the lack of detail in Count One, it is impossible to discern which, if any, particular computer . . . Singla is

---

<sup>1</sup> The law-of-the-case doctrine provides that courts are “bound by findings of fact and conclusions of law” previously made in the same case unless “(1) a subsequent trial produces substantially different evidence, (2) controlling authority has since made a contrary decision of law applicable to that issue, or (3) the prior decision was clearly erroneous and would work manifest injustice.” *United States v. Stinson*, 97 F.3d 466, 469 (11<sup>th</sup> Cir.1996). *United States v. Victores*, 402 F. App'x 465, 466–67 (11<sup>th</sup> Cir. 2010). Mr. Singla argues that his doctrine is only applicable to rulings issued by appellate courts. [Doc. 84 at 4]. Although it is indeed the case that this doctrine is not typically applicable at the current stage of this litigation, the undersigned will abide by the District Court’s ruling on this claim.

under indictment for having allegedly damaged[.]” (Doc. 68 at 10.) The original and renewed motions make the same argument.” [*Id.*].

This Court agrees. In reference to Count one, the District Court issued this ruling:

Defendant Singla has adequate information to defend against the allegation that, on September 27, 2018, he transmitted a program or command to the computers used by the Gwinnett Medical Center to operate the Ascom phone system at the Duluth Hospital. Following the resolution of this case, the indictment allows him to plead double jeopardy to bar any subsequent allegation that, on that day, he sent a program or command to try to damage those computers. The United States has followed the Supreme Court’s instructions in *Hamling* as to the detail it must include in Count One. The Court sustains the United States’s objection to that finding in the Report and Recommendation.

[Doc. 63 at 7].

The District Court also concluded that:

[t]he allegations in Counts Two through Seventeen identify the exact computers Defendant is alleged to have damaged or tried to damage and the day he is alleged to have done so. They allow him to prepare his defense and protect against any subsequent prosecution for the same conduct. They pass constitutional muster, and the Court sustains the United States’s objection to the Magistrate Judge’s conclusion the indictment fails to identify adequately the computers at issue in these counts.

[*Id.* at 9].

Although Mr. Singla maintains that his renewed claim is not based on the same constitutional challenge he previously raised, his prior and current claims are

grounded on the same alleged pleading error: that the language in those counts fail to adequately identify the specific “protected computer” he allegedly damaged and that this ambiguity prevents him from raising due process claims. Accordingly, this Court will not re-consider this constitutional challenge and will turn to Mr. Singla’s remaining claims.

In his second claim, Mr. Singla asserts that the Government’s failure to identify at least one unique “protected computer” in the felony-loss provision of Section 1030(c)(3)(I), renders Counts One through Seventeen constitutionally infirm. [Doc. 68 at 13]. This provision authorizes an increased sentence if the offense caused (or would have caused if completed):

loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least \$5,000 in value [.]

18 U.S.C. § 1030(c)(3)(I).

Mr. Singla submits that the Government has misread this enhancement provision, mistakenly believing it only needs to prove one of two factual predicates to justify application of the enhancement. [Doc. 68 at 11]. He argues that the statute requires proof of loss to at least one person and loss affecting at least one other “protected computer.” [*Id.*]. Because of the Government’s misinterpretation of the



statute, Mr. Singla argues, he risks being punished twice for “damage” caused to only one “protected computer.” [Doc. 68 at 12]. He also claims that a merger problem<sup>2</sup> could arise if the Government relies on the same facts to support the underlying violation of Section 1030(a)(5)(A) and the enhancement provision; a fatal drafting error that renders these charges unconstitutional. [Doc 68 at 12].

The Government urges this Court to reject this claim as well. It asserts that Mr. Singla’s argument is based on a flawed interpretation of the statute. [Doc. 73 at 10-11]. Citing *Lanam v. United States*, 554 F. App’x 413, 417 (6<sup>th</sup> Cir. 2014), it submits that 18 U.S.C. Section 1030(a)(5)(B)(i) “requires only a total loss of \$5,000, which can be aggregated based on the conduct charged along with any relevant course of conduct during a 1-year period.” [*Id.* at 11]. The Government also relies on Eleventh Circuit Pattern Jury Instruction 42.3 (2020) which provides, in part, that damage to a protected computer includes: “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.” Therefore, it

---

<sup>2</sup> A merger problem is “tantamount to double jeopardy,” *United States v. Santos*, 553 U.S. 507, 527, (2008) (Stevens, J., concurring), where the facts or transactions alleged to support one offense are also used to support another.

submits that the relevant amount of loss justifying this enhancement is properly based on Mr. Singla's entire course of conduct against the "protected computers" – "either from the damaged protected computers that were the direct subject of the charge or from related (and necessarily other) protected computers." [Doc. 73 at 13]. Additionally, the Government argues that this claim is prematurely alleged, asserting that any concerns regarding a merger violation should be raised at the conclusion of the trial. [*Id.*].

The plain language of the statute supports the Government's position. An examination of this provision clearly states that the applicable loss amount can be based on an aggregation of the loss caused by a defendant's entire course of conduct. "As with any question of statutory interpretation, we begin by examining the text of the statute to determine whether its meaning is clear." *Lewis v. Barnhart*, 285 F.3d 1329, 1331 (11<sup>th</sup> Cir.2002); See Also, *Merritt v. Dillard Paper Co.*, 120 F.3d 1181, 1185 (11<sup>th</sup> Cir.1997) ("In construing a statute we must begin, and often should end as well, with the language of the statute itself."). Furthermore, "[t]he plainness or ambiguity of statutory language is determined [not only] by reference to the language itself, [but as well by] the specific context in which that language is used, and the broader context of the statute as a whole." *Yates v. United States*, 574

U.S. 528, 537 (2015) (alterations in original) (quoting, *Robinson v. Shell Oil Co.*, 519 U.S. 337, 341 (1997)).

As noted by the Government, this provision specifically identifies the potential harm one could cause to multiple “protected computers” during an extended criminal episode. Mr. Singla’s strained interpretation of this provision is not supported by Circuit precedent and creates ambiguity where none exists. Thus, the undersigned concludes that the loss-enhancement charges are properly alleged. The Court also agrees that any merger problem can be timely raised following trial or on appellate review.

Mr. Singla’s final constitutional claim alleges that the Government’s failure to identify the particular “program, information, code, or command” and the alleged “damage” caused by the “transmissions” renders Counts One through Seventeen constitutionally infirm. [Doc. 68 at 13]. Because the Indictment merely recites the “bare and conclusory” language of the statute without providing “enough facts and circumstances to inform [him] of the specific offense being charged,” he submits, they are unconstitutionally vague, prohibiting him from pleading double jeopardy, and allowing the Government to rely on “shifting theories and evidence on these elements in the grand jury, at trial, and on appeal.” [*Id.* at 15.]. He also argues that the due process clause requires that these counts allege how each “protected

computer” was damaged, whether by “disabling or overwhelming a server or program, or corrupting or destroying a file or data”. [Doc. 68 at 13]. By simply tracking the general terms of the statute, he argues, he has not been sufficiently apprised of the facts and circumstances surrounding the charged offenses. [*Id.* at 14].

The Government argues these allegations are also unfounded because the Indictment specifically informs Mr. Singla that he knowingly caused “the conveyance of a program, information, code or command from one place to another.” [Doc. 73 at 15]. It submits that the language of the Indictment comports with notice requirements that due process demands and utilizes terms specifically defined by the CFAA. [*Id.* at 15-16]. And although the Indictment does not specify the particular “transmission, program, code or command” that caused “damage” to the “protected computers,” the Government maintains that “settled law of notice pleading in criminal cases” does not require the inclusion of additional facts. [*Id.* at 16].

As for the “damage” element, the Government submits that Mr. Singla’s assertion that the Indictment must include a description of the type of “damage” caused by the transmission of the code or program reflects his misunderstanding of its constitutional obligations. [Doc. 73 at 19-20]. It claims that this term is defined

in the CFAA which provides sufficient notice of the type of harm the statute proscribes. [*Id.*]. Further, the Government states that “[t]he grand jury’s return of the indictment provides a conclusive determination that they were presented facts showing probable cause that Singla intentionally caused damage to the protected computers identified in Counts One through Seventeen.” [Doc. 73 at 20]. The definitions provided in the statute, coupled with Mr. Singla’s apparent knowledge of the nature of the offenses based on “his very assertion of constitutional infirmity,” undermine any legitimate claim that the Indictment is unconstitutionally insufficient. [*Id.* at 20].

The Government’s arguments are unpersuasive. First of all, although the pending Indictment sets forth 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); *United States v. Bobo*, 344 F.3d 1076, 1083 (11<sup>th</sup> Cir. 2003).

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, concluding that 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.

In an attempt to establish that the pending Indictment is factually sufficient, the Government submitted indictments that have been returned in other cases charging violations of the CFAA. [Doc. 53; Ex. B, C, D, E]. All of these indictments

allege that the defendants caused the “transmission of a program, code, and command” that damaged “protected computers.” However, unlike the pending Indictment, each of these indictments contain specific details of the defendants’ alleged conduct that violated the CFAA. For example, the indictment in *United States v. Vascho-DesJardins*, states that the defendant “did knowingly cause the transmission of a program, information, code and command – that is, a program, information, code and command related to a NetWalker Ransomware attack on a victim company located in Tampa, Florida.” [Doc. 53-3; Ex. C].

In *United States v. Gasperini*, the indictment includes a twelve-paragraph introductory section that describes the nature of the alleged offenses and the harm the defendant caused, explaining that a “botnet” is “a network of computers (such as servers) infected with malicious software without the users’ knowledge or authorization. A malicious actor can remotely control the computers (which are described individually as “bot”) and draw upon the bandwidth and computing power of the individual bots for many malicious purposes including to launch denial-of-service attacks, deliver large-scale spam campaigns, transmit viruses or spyware, steal banking credentials or personally identifiable information, perform far-reaching vulnerability scans, perpetrate click fraud, and engage in other acts of cybercrime.” [Doc 53-2; Ex. B]. The *Gasperini* indictment also states that the

defendant, “together with others, accessed the compromised servers without permission and installed on them malicious software that gave him remote access to, and control of, these compromised servers, which together constituted a botnet.” [*Id.* at 3]. Further, this indictment alleges that the defendant installed malicious computer scripts on the compromised servers that caused them to execute specific commands. [*Id.*]

The indictment in *United States v. Hutchins* also provides a detailed description of the overt acts the defendant allegedly committed, stating that he “hacked control panels associated with phase Bot, malware [defendant] perceived to be competing with Kronos. In a chat with Individual B, [defendant] stated, ‘well we found exploit (sic) in his panel just hacked all his customers and posted it on my blog sucks that these [ ] idiots who cant (sic) code make money off this: [defendant] then published an article on his Malwaretech blog titled ‘Phase Bot – Exploiting C&C Panel’ describing the vulnerability.” [*Id.* at 5].

Finally, although the indictment in *United States v. Savu* does not identify the particular program or code that the defendant allegedly caused to be transmitted, it reveals that the victim companies’ protected computers allowed for public access but that its networks could only be accessed by imputing “with unique credentials, which included a username and password.” [Doc. 53-5; Ex. E].



The specificity of the facts and circumstances provided in these cases stands in stark contrast to the sparse information contained in the pending Indictment. It simply parrots the general language of the CFAA. It does not identify the particular “program, information, code, and command” Mr. Singla allegedly utilized, nor does it describe the type of “damage” his conduct caused to the “protected computers.” “[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.” *Russell*, 369 U.S. at 761 (1962). *Id.* at 765 (citing, *United States v. Cruikshank*, 92 U.S. 542, 558 (1875)). Because of these omissions, the Indictment fails to adequately inform him of the nature of the offenses he allegedly committed, rendering them unconstitutionally vague. See, *United States v. Peterson*, 544 F. Supp. 2d 1363, 1375 (M.D. Ga. 2008) (where charges were dismissed upon court’s finding that the indictment was “so vague and the meaning of the statutory terms are so broad, it does not sufficiently apprise Defendant of what he must be prepared to meet, and therefore, it is factually insufficient.”); *United States v. Tripodis*, No. 1:18-CR-240-1-TWT-JFK, 2020 WL 914681 (N.D. Ga., Feb. 26, 2020)(where court found several counts unconstitutionally vague because the indictment did not “apprise the Defendant with reasonable certainty of the nature of accusations against

him.”). cf., *United States v. Hutchins*, 361 F. Supp. 3d 779, 793 (E.D. Wisc., Feb. 11, 2019)(where court found indictment charging defendant with violations of the CFAA was not unconstitutionally vague. 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.).

Although the Government has previously provided discovery that includes numerous investigative reports, summaries of interviews and data supplied by GMC [Doc. 78], this Court’s determination of whether the Indictment comports with the notice requirement of the Sixth Amendment is limited to an examination of the four corners of the Indictment. *Salman, supra*, 378 F.3d at 1268 (“the sufficiency of a criminal indictment is determined from its face.”). Moreover, a bill of particulars cannot cure these constitutional deficiencies. *Russell, supra*, 369 U.S. at 769-70.

Because the Indictment fails to sufficiently inform Mr. Singla of the facts and circumstances surrounding the charged offenses, this Court finds that Counts One through Seventeen are unconstitutionally vague in violation of the Sixth Amendment. Accordingly, the undersigned **RECOMMENDS** that the Motion to Dismiss Indictment for Lack of Specificity be **GRANTED**.

**B. Defendant’s Renewed Motion to Dismiss Count Eighteen of the Indictment as Unconstitutionally Vague**

Mr. Singla makes both facial and as-applied challenges to §1030(a)(2)(C). Before turning to the merits of these claims, it is important to clarify at the outset the type of showing required. “A facial challenge, as distinguished from an as-applied challenge, seeks to invalidate a statute or regulation itself.” *United States v. Frandsen*, 212 F.3d 1231, 1235 (11th Cir. 2000). In other words, as noted by the Government, a facial challenge does not attack a *particular* application of a statute, but all *possible* applications. See, *Jacobs v. The Florida Bar*, 50 F.3d 901, 906 n.20 (11<sup>th</sup> Cir. 1995) (“[W]hen a plaintiff attacks a law facially, the plaintiff bears the burden of proving that the law could never be constitutionally applied.”). It is “the most difficult challenge to mount successfully” because it requires a defendant to show “that no set of circumstances exists under which the [law] would be valid.” *United States v. Salerno*, 481 U.S. 739, 745 (1987); *see also Frandsen*, 212 F.3d at 1235 (stating that “no set of circumstances” is the general rule for evaluating facial challenges in the Eleventh Circuit). Because Mr. Singla has not met this burden, his facial challenge cannot succeed. *See Salerno*, 481 U.S. at 745; *Frandsen*, 212 F.3d at 1235. Accordingly, the undersigned **RECOMMENDS** that Defendant’s Motion to Dismiss be **DENIED** as to his facial challenge. The undersigned now turns to Mr. Singla’s as-applied challenge.

## Discussion

Pursuant to the Due Process Clause of the Fifth Amendment, a statute or regulation is “void for vagueness if its prohibitions are not clearly defined.” *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972); *Keister v. Bell*, 29 F. 4<sup>th</sup> 1239 (11<sup>th</sup> Cir. 2022). Unconstitutionally vague laws fail to provide “fair warning” of what the law requires, and they encourage “arbitrary and discriminatory enforcement,...if arbitrary and discriminatory enforcement is to be prevented, laws must provide explicit standards for those who apply them.” *Grayned*, at 108. Thus, the void-for-vagueness doctrine requires that a penal statute define a criminal offense with such specificity that “ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement.” *Village of Hoffman Estates v. Flipside*, 455 U.S. 489 (1982); *Connally v. General Construction Co.*, 269 U.S. 385 (1926). When the legislature fails to provide these minimal guidelines, a criminal statute may permit “a standardless sweep [that] allows policemen, prosecutors, and juries to pursue their personal predilections.” *Smith v. Goguen*, 415 U.S. 566, 575 (1974); *Kolender v. Lawson*, 461 U.S. 352, 357–58 (1983). Furthermore, “[t]he...principle is that no man shall be held criminally responsible for conduct which he could not reasonably

understand to be proscribed.” *Bouie v City of Columbia*, 378 U.S. 347 (1964), quoting, *United States v. Harriss*, 347 U.S. 612, 617 (1954).

In the instant case, Count Eighteen alleges that: “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.” [Doc. 1 at 5]. Mr. Singla submits that this Count must be dismissed because the charged offense ““fails to provide a person of ordinary intelligence fair notice of what is prohibited” and ‘is so standardless that it authorizes or encourages seriously discriminatory enforcement.’” [Doc. 86 at 1]. However, this Court cannot consider the merits of this challenge because the record is incomplete. Because a factual, as-applied challenge “asserts that a statute cannot be constitutionally applied in particular circumstances, it necessarily requires the development of a factual record for the court to consider.” *Harris v. Mexican*

*Specialty Foods, Inc.*, 564 F.3d 1301, 1308 (11<sup>th</sup> Cir. 2009). This is because an as-applied challenge “addresses whether ‘a statute is unconstitutional on the facts of a particular case or to a particular party.’” *Schultz v. Alabama*, 42 F.4th 1298, 1319 (11<sup>th</sup> Cir. 2022), cert. denied sub nom. Hester v. Gentry, No. 22-835, 2023 WL 3937613 (U.S. June 12, 2023); See Also, *Williams v. Pryor*, 240 F.3d 944, 955 (11<sup>th</sup> Cir. 2001) (“We remand the as-applied challenges for due consideration by the district court because the record and stipulations in this case simply are too narrow to permit us to decide whether or to what extent the Alabama statute infringes a fundamental right to sexual privacy of the specific plaintiffs in this case.”). Therefore, this Court **DEFERS** this motion to permit review by the District Court following completion of the record at trial.

### **C. Defendant’s Renewed Motion for Bill of Particulars**

Mr. Singla seeks a bill of particulars because he alleges that the Indictment “fails to provide facts sufficient to enable [him] to prepare his defense and avoid the possibility of prejudicial surprise at trial.” [Doc. 71 at 1]. As to Count One, he requests: (1) identification of the particular “protected computer” described in Count One or the other protected computer that supports the felony-loss in Paragraph 3a; (2) evidence revealing the transmission of any “program, information, code, or command” that caused the Ascom system to malfunction; (3) information

that establishes that the protected computers (including the Ascom phone system) were connected to the internet at the time the offenses were committed in order to determine whether the computers and GMC's phone system had been "used in or affected[ed] interstate or foreign commerce or communication"; (4) the specific amounts and types of losses suffered based on Mr. Singla's alleged damage to the protected computers; and (5) information describing the actual or potential impact the offenses had on patient care. [Doc. 71 at 9-12]. He submits that although the Government has revealed that the "protected computer" described in this Count is the Ascom phone system, the discovery he has been provided "relates to a multitude of devices" and "does not appear to answer these specific questions." [*Id.* at 9-10]. He makes similar requests for Counts Two through Eighteen, asserting that this information is essential to the preparation of his defense. [*Id.* at 13]. As to Count Eighteen, he requests that the Government identify the particular computer he allegedly accessed without authorization, the nature of his unauthorized access or how he exceeded authorized access, and how the "protected computer" in this Count was used in or affected interstate commerce. [*Id.* at 14-16]. He argues that all of these particulars are necessary to allow him to properly defend himself, provide relevant data to his experts in anticipation of trial and to prevent prejudicial surprise. [*Id.* at 10,16].

The Government objections to all of these requests, asserting that the information Mr. Singla seeks is “outside the scope of a bill of particulars and has already been provided in the Indictment and discovery.” [Doc. 77 at 12]. It also claims that these requests would compel the revelation of its “order of proof and its legal theories,” disclosures not mandated by Circuit precedent nor Fed. R. Crim. Proc. 7(f). [Doc. 77 at 25].

### **Discussion**

Rule 7 of the Federal Rules of Criminal Procedure authorizes a court to direct the Government to file a bill of particulars. FED. R. CRIM. P. 7(f). “The purpose of a bill of particulars is to inform the defendant of the charge against him with sufficient precision to allow him to prepare his defense, to minimize surprise at trial, and to enable him to plead double jeopardy in the event of a later prosecution for the same offense.” *United States v. Warren*, 772 F.2d 827, 837 (11<sup>th</sup> Cir. 1985); *United States v. Cole*, 755 F.2d 748 (11<sup>th</sup> Cir. 1986). “A request for bill of particulars is, inter alia, befitting in those instances where the defendant seeks further clarity and precision with regard to the charges that he is facing in order to adequately prepare a defense.” *Warren*, 772 F.2d at 837. However, “generalized discovery is not the proper function of a bill of particulars.” *Id.*



This Court has broad discretion in ruling on requests for bills of particular. *Will v. United States*, 389 U.S. 90 (1967). A defendant is not entitled to a bill of particulars “with respect to information which is already available through other sources such as the indictment or discovery and inspection.” *United States v. Rosenthal*, 793 F.2d 1214, 1227 (11<sup>th</sup> Cir. 1986), *modified on other grounds by*, 801 F.2d 378 (11<sup>th</sup> Cir. 1986). Furthermore, a bill of particulars may not be used for the purpose of obtaining detailed disclosure of the government’s case or its evidence in advance of trial. *See United States v. Perez*, 489 F.2d 51, 70-71 (5<sup>th</sup> Cir. 1973).<sup>3</sup> Moreover, it “cannot be used as a weapon to force the government into divulging its prosecution strategy; we do not allow defendants to ‘compel the government to detailed exposition of its evidence or to explain the legal theories upon which it intends to rely at trial’ in that manner.” *United States v. Burgin*, 621 F.2d 1352, 1359 (5<sup>th</sup> Cir. 1980); *United States v. Maurya*, 25 F.4th 829, 837–38 (11<sup>th</sup> Cir. 2022).

In the instant case, Mr. Singla submits that the requested particulars are necessary in light of the complexity of the CFAA and the Indictment’s lack of precision based on its use of general and conclusory terminology. [Doc. 85 at 1]. He

---

<sup>3</sup> In *Bonner v. City of Prichard*, 661 F.2d 1206 (11<sup>th</sup> Cir. 1981) (*en banc*), the Eleventh Circuit adopted as binding precedent all decisions rendered by the Fifth Circuit before October 1, 1981.

also contends that he is not attempting to obtain the Government's legal theories; "he simply needs more particularized information about the charges against him." [*Id.* at 5].

The Government maintains that all of Mr. Singla's requests should be denied because they are either beyond the scope of a bill of particulars or the information has already been provided. [Doc. 77 at 15, 17, 19, and 24]. Regarding Count One, it submits that it has already identified (and the District Court affirmed) the "protected computer" as the Ascom phone system. [*Id.* at 15]. It also claims that the requests related to the statutory elements "transmission," "interstate commerce," "loss," and "modification or impairment" should be denied because all of this information has been previously disclosed; specifically identifying the BATES stamped documents it provided to Mr. Singla. [*Id.* at 18, 19, and 21]. This Court agrees. Although Mr. Singla may prefer more comprehensive information regarding Count One, a bill of particulars "is not designed to compel the government to detailed exposition of its evidence or to explain the legal theories upon which it intends to rely at trial." *United States v. Roberts*, 174 Fed. Appx. 476, 477 (11<sup>th</sup> Cir. 2006), quoting, *Burgin*, 621 F.2d at 1359.

As for Mr. Singla's requests related to Counts Two through Seventeen, the Government again submits that it has already provided this information to Mr.

Singla. [Doc. 77 at 17 – 20]. Specifically, it states that the request for the “transmission” is unwarranted because it was already revealed (“the screenshot of the string...baidu”). [*Id.* at 18]. His request for information regarding the “damage” element is also unnecessary, it argues, because the discovery identifies the damage caused when the network printers were attacked: “the attack on the network printers caused patient health information and the threatening message ‘WE OWN YOU!’ to be printed from the network printers. (FBI-000002)”. [*Id.* at 19]. As for the “loss” element, the Government notes that Mr. Singla conceded that he was provided a line-item summary of the losses suffered by GMC. [*Id.* at 20].

The Government also argues that Mr. Singla has been informed of the impact the cyberattack had on patient care (related to the “modification or impairment” element) that occurred as a result of the damage caused to the Ascom phone system. [*Id.* at 21]. This information reveals that the phone system was “critical for patient care” and that the unlawful interference with the network printers caused them to be “pulled for quarantine and review.” [*Id.*]. Based on these disclosures, the Government claims that Mr. Singla is not entitled to any additional discovery. This Court agrees.

The Government also submits that the requests related to Count Eighteen are unwarranted. [Doc. 77 at 22]. It claims Mr. Singla is on notice of the facts

supporting this Count because the “protected computer” he utilized has been identified as the Hologic R2 Digitizer, information that “renders the existence of any other computer legally irrelevant because that device is both the “protected computer” and the computer from which [he] accessed and obtained information.” [Doc. 77 at 22]. Although Mr. Singla disagrees with the Government’s interpretation of the statute in this context, the Government has provided its answer.

The Government also claims that Mr. Singla cannot feign surprise regarding his professional association with GMC or the boundaries of his access to its communications system, asserting that: “GMC did not employ Singla. GMC had no business with Singla. Singla had no lawful reason to be on the GMC network. Nor did Singla have lawful reason to obtain GMC patient health information and publish it on Twitter.” [Doc. 77 at 23]. It also states that Mr. Singla knows that the Ascom phone system was connected to the internet, citing the BATES stamped document that describes the system’s WiFi capabilities. [*Id.* at 24].

Because the Government has provided Mr. Singla with the information he requests, he has failed to establish that a bill of particulars is required to allow him to prepare his defense, minimize the risk of prejudicial surprise, or prevent him from pleading double jeopardy in the future. See, *United States v. Cantu*, 557 F.2d 1173, 1178 (5<sup>th</sup> Cir.1977)(holding that where the evidence consists mainly of testimony by

witnesses of conversations in which the defendant participated, of activity occurring in defendant's place of business that he observed, and of arrests in the business parking lot which he witnessed, he “could hardly have been surprised by the government's proof at trial.”)(citations omitted). Accordingly, the Motion for a Bill of Particulars is **DENIED**.

**D. Defendant’s Renewed Motion for Early Issuance of Rule 17(c) Subpoena**

Pursuant to Fed. R. Rule 17(c), Mr. Singla moves this Court for early issuance of a subpoena for the following information:

- Firewall activity logs respecting any GMC computer or device alleged in the Indictment during the 2018 incident.
- Any report of PwC (or of any other breach response or breach Remediation consultant or expert) on the causes of the 2018 incident, any damage caused by the 2018 incident to equipment or software, steps taken to correct or address such damage and replace or repair such equipment or software, detailed information regarding the costs thereof, or notes, presentations, or workpapers functioning as the equivalent of such report.
- Documents concerning any cybersecurity incidents at GMC prior to the 2018 incident.
- Detailed information regarding GMC’s breach response and remediation expenses, costs, or fees in connection with any investigation into the 2018 incident, including but not limited to receipts, invoices, billing narratives, payment records, and related correspondence concerning work performed for GMC by King & Spalding LLP, PwC, and other consultants and vendors relating to the 2018 incident.

[Doc. 83].

Because of the “highly technical nature” of the evidence in this case, Mr. Singla submits that early disclosure of this information is necessary to allow him to prepare his defense, enable his experts to examine the documents in anticipation of trial, and avoid delaying trial. [Doc. 83 at 6]. The Government objects to this request, arguing that this subpoena is improper because Mr. Singla seeks to use it as a discovery tool rather than a particularized request for relevant and admissible evidence. [Doc. 74 at 7]. Because it believes these requests consist of “a fishing expedition at the expense of the victim hospital system,” it submits that the motion should be denied. [*Id.*].

### **Discussion**

Fed. R. Crim. Pro. 17(c)(1) provides: “A subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates. The court may direct the witness to produce the designated items in court before trial or before they are to be offered in evidence.” In order to obtain production prior to trial under Rule 17(c), the moving party must show:

- (1) that the documents are evidentiary and relevant; (2) that they are not otherwise procurable reasonably in advance of trial by exercise of due diligence; (3) that the party cannot properly prepare for trial without such production and inspection in advance of trial and that the

failure to obtain such inspection may tend unreasonably to delay the trial; and (4) that the application is made in good faith and is not intended as a general “fishing expedition.”

*United States v. Nixon*, 418 U.S. 683, 699-700 (1974).

The Due Process Clause of the Fourteenth Amendment requires that a criminal defendant “be afforded a meaningful opportunity to present a complete defense.” *California v. Trombetta*, 467 U.S. 479, 485 (1984). “To safeguard that right, the Court has developed ‘what might loosely be called the area of constitutionally guaranteed access to evidence....’ [T]his group of constitutional privileges delivers exculpatory evidence into the hands of the accused, thereby protecting the innocent from erroneous conviction and ensuring the integrity of the criminal justice system.” *Id.* (citations omitted). Nevertheless, “[t]he right to defend oneself does not extend to using the power of the Court to compel third parties to provide information that may not even be admissible at trial or at a hearing or that is merely ‘investigatory.’” *United States v. Rand*, 835 F.3d 451, 463, (11<sup>th</sup> Cir. 2016)(citations omitted); *United States v. Winner*, No. CR 117-034, 2018 WL 1998311, at \*1–2 (S.D. Ga. Apr. 27, 2018).

Furthermore, Rule 17 expedites “the trial by providing a time and place before trial for the inspection of subpoenaed materials.” *Nixon*, 418 U.S. at 698-99. However, the party requesting production must “clear three hurdles: (1) relevancy;

(2) admissibility; (3) specificity.” *Id.* at 700. “Courts have noted that the specificity and relevance elements are somewhat heightened in that they ‘require more than the title of a document and conjecture as to its contents.’” *United States v. Brown*, No. 11-60285, 2013 WL 1624205, at \*4 (S.D. Fla. Apr. 15, 2013) (Rosenbaum, J.) (citing *United States v. Arditti*, 955 F.2d 331, 345 (5<sup>th</sup> Cir. 1992)). Furthermore, “[a]s the Eleventh Circuit has explained, ‘the rule only reaches *specifically identified documents* that will be admissible as evidence at trial, provided that the application for the subpoena is made in good faith.’” *Id.* (citation omitted)(emphasis added).

Moreover, this Rule is “not intended to provide an additional means of discovery for any party in criminal cases.” *United States v. Silverman*, 745 F.2d 1386, 1397 (11<sup>th</sup> Cir. 1984) (citing *Bowman Dairy Co. v. United States*, 341 U.S. 214, 220 (1951)). Nor can it be used “as a means for developing investigative leads which would lead to evidence producible at trial.” *United States v. Noriega*, 764 F. Supp. 1480, 1492 (S.D. Fla. 1991).

As stated above, Mr. Singla seeks four categories of information: (1) Firewall activity logs respecting any GMC computer or device alleged in the Indictment during the 2018 incident; (2) Any report of PwC (or of any other breach response or breach Remediation consultant or expert) on the causes of the 2018 incident, any damage caused by the 2018 incident to equipment or software, steps taken to correct



or address such damage and replace or repair such equipment or software, detailed information regarding the costs thereof, or notes, presentations, or workpapers functioning as the equivalent of such report; (3) Documents concerning any cybersecurity incidents at GMC prior to the 2018 incident and (4) Detailed information regarding GMC's breach response and remediation expenses, costs, or fees in connection with any investigation into the 2018 incident, including but not limited to receipts, invoices, billing narratives, payment records, and related correspondence concerning work performed for GMC by King & Spalding LLP, PwC, and other consultants and vendors relating to the 2018 incident. [Doc. 67].

Mr. Singla argues that the first category of documents – the firewall activity logs – are critical pieces of evidence in any cybersecurity incident and that it's standard procedure "in every remediation investigation for them to be collected and reviewed, and the logs contain information that will exculpate [him]." [Doc. 67 at 6]. The Government objects to this request because it has already informed Mr. Singla that neither it nor GMC are in possession of these records. [Doc. 74 at 8]. Despite this explanation, Mr. Singla requests that this Court order GMC to produce these documents or formally confirm that they were either destroyed or were not preserved. Because Mr. Singla has been informed that these documents are not in

the possession of GMC, there is no good faith basis for issuance of a subpoena for these records.

Mr. Singla claims that the third category of documents he seeks – *any* cybersecurity incidents at GMC prior to the 2018 incident – is needed to ensure that the alleged damage to GMC’s devices was not caused by another bad actor in a prior cyberattack. However, as noted by the Government, this request “is aimlessly overbroad.” [Doc 74 at 9]. Because this request lacks specificity and is of limited relevancy given Mr. Singla’s mere assumption that GMC previously suffered the same harm alleged in the instant case, issuance of a subpoena for this information is unwarranted. See, *United States v. Cole*, 755 F.2d 748, 759 (11<sup>th</sup> Cir. 1985)(holding that unsubstantiated allegations do not satisfy the particularized need standard).

The same holds true for Mr. Singla’s two remaining requests. The second request seeks “any report of PwC (or of any other breach response or breach remediation consultant or expert) on the causes of the 2018 incident.” [Doc. 67 at 7]. It also seeks “notes, presentations, or workpapers functioning as the equivalent of such report.” This request is so broad that it fails to comport with the requirement that the subpoena target “specifically identified documents.” *Arditti, supra*, 955 F.2d 331.

The final request is doomed for the same reason. It seeks “detailed information” regarding GMC’s breach response and remediations expenses. [Doc. 67 at 9]. But it doesn’t stop there. Mr. Singla also seeks “receipts, invoices, billing narrative, payment records and related correspondence” concerning work performed by GMC’s attorneys, consultants, and vendors. [*Id.*]. The breadth of this request could arguably include attorney/client privileged materials, emails and text messages; so broadly drafted that it fails to meet the specificity standard Rule 17 requires. See, *United States v. Winner*, No. CR 117-034, 2018 WL 1998311, at \*2–3 (S.D. Ga. Apr. 27, 2018)(where the court approved only one of forty requested subpoenas, finding the vast majority were “scattershot, dragnet attempts to discover evidence not presently known to exist.”). Accordingly, the Motion for Early Issuance of Rule 17(c) Subpoena is **DENIED**.

#### **D. Defendant’s Renewed Motion to Compel Disclosure of Grand Jury Transcripts**

Mr. Singla moves this Court to compel disclosure of grand jury transcripts because he believes the Government failed to properly instruct and advise the grand jurors as to the applicable law and facts regarding these elements of the CFAA: “protected computer,” “transmission,” and” damage.” [Doc. 70 at 3]. In order to determine whether the Government’s alleged erroneous interpretation of key provisions of the CFA adversely affected the grand jury’s proceedings, he avers

disclosure is justified. [Doc. 87 at 8]. He also believes that Government's witnesses "misled or confused the grand jury about such facts, and thus that [his] indictment is unconstitutional and invalid." [*Id.* at 5]. Therefore, he requests disclosure of the transcripts or, in the alternative, *in camera* review of these documents by the undersigned to determine whether disclosure is appropriate.

The Government opposes this request, characterizing Mr. Singla's request as simply a "fishing expedition" proscribed by Rule 6(e) of the Federal Rules of Criminal Procedure. [Doc. 75 at 3]. It also argues that because Mr. Singla cannot demonstrate a "particularized need" for these transcripts, Circuit precedent does not require disclosure. [*Id.* at 5-6].

### **Discussion**

"It has been a long-standing policy of the law that grand jury proceedings should be kept secret and only disclosed in limited circumstances." *United States v. Aizenberg*, 358 F.3d1327, 1346 (11<sup>th</sup> Cir. 2004). Federal Rule of Criminal Procedure 6(e) generally prohibits the disclosure of grand jury material. This rule specifically states that "the following persons must not disclose a matter occurring before the grand jury:(i) a grand juror; (ii) an interpreter; (iii) a court reporter;(iv) an operator of a recording device;(v) a person who transcribes recorded testimony; (vi) an attorney for the government; or (vii) a person to whom disclosure is made under

Rule 6(e)(3)(A)(ii) or (iii).” Fed. R. Crim. P. 6(e)(2)(B). Rule 6(e)(3), however, provides for several exceptions under which this Court may authorize disclosure of grand jury materials. In particular, disclosure of the following matters could be ordered:

- (i) preliminarily to or in connection with a judicial proceeding; [or]
- (ii) at the request of a defendant who shows that a ground may exist to dismiss the indictment because of a matter that occurred before the grand jury[.]

Fed. R. Crim. P. 6(e)(3)(E)(i)-(ii); *United States v. Davis*, 721 F. App'x 856, 860 (11<sup>th</sup> Cir. 2018).

These exceptions only apply when the moving party establishes “a particularized need” for that material. *See Douglas Oil Co. of Cal. v. Petrol Stops Nw.*, 441 U.S. 211, 222–24 (1979). To meet this standard, the moving party must show that he needs this material to avoid “a possible injustice in another judicial proceeding, that the need for disclosure is greater than the need for continued secrecy, and that his request is structured to cover only material so needed.” *Id.* at 222. The Eleventh Circuit has held that “that a party meets a particular need standard when he shows that circumstances created certain difficulties peculiar to his case which could be alleviated by access to specific grand jury material, without

doing disproportionate harm to the statutory purpose embodied in the grand jury process.” *Aisenberg*, 358 F.3d at 1348–49. Unsubstantiated allegations do not satisfy this particularized need standard. *United States v. Cole*, 755 F.2d 748, 759 (11<sup>th</sup> Cir. 1985); *Beiter v. United States*, No. 22-12282, 2023 WL 1980773, at \*2 (11<sup>th</sup> Cir. Feb. 14, 2023). Thus, the party seeking disclosure bears the heavy burden of establishing a “compelling necessity” for disclosure. *United States v. Proctor & Gamble Co.*, 356 U.S. 677, 683 (1958). Moreover, “a blanket request for all grand jury materials cannot be described as the kind of particularized request required for the production of otherwise secret information.” *Aisenberg*, 358 F.3d at 1349.

In the instant case, Mr. Singla moves for disclosure of the following material: (1) transcripts of the prosecutors’ instructions to the grand jury and any physical documents provided to the grand jury that constitute such instructions, (2) transcripts of the prosecutors’ advice and explanation of such instructions to the grand jury, (3) transcripts of testimony of any witness on the “protected computer,” “transmission,” and “damage” elements, and (4) any exhibits or other documents provided to the grand jury that are necessary to understand said testimony relevant to the “protected computer,” “transmission,” and “damage” elements. [Doc. 70 at 8]. He claims that he has established a particularized need for the grand jury transcripts because the pretrial briefing, the Government’s legal arguments presented during

oral arguments, and the nature of the allegations in the Indictment, demonstrate the Government's erroneous interpretation of the CFAA. [*Id.* at 1-2]. This misinterpretation, he surmises, proves that the grand jury "must have" been misinstructed regarding the statute's elements. [Doc. 70 at 1-2]. He also argues that the Indictment's omission of the term "other" in the felony-loss provision outlined in Paragraph 3a of Count One and Paragraph 5 of Counts Two through Seventeen, a term that denotes that this enhancement must be supported by a "protected computer" "that is different from the one upon which each underlying count is predicted,...confirms that the grand jury must have been misinformed or misled, bolstering [his] showing of particularized need" for the transcripts. [Doc. 70 at 6]. Mr. Singla also offers legal authority from the Ninth Circuit where those courts authorized disclosure of jury instructions based on their conclusion that prohibition on disclosure was inapplicable because the instructions were considered "ministerial" rather than "substantive" materials that Rule 6(e) protects from disclosure. [*Id.* at 8-9].

The Government submits that Mr. Singla's reliance on non-binding Ninth Circuit precedent is unpersuasive because these cases are factually inapposite. [Doc. 75 at 16-17]. It also claims that Mr. Singla's assertion that the grand jury was misinformed on the applicable law and relevant facts is purely speculative. [Doc. 75

at 16-17]. The Government emphasizes the strong presumption “beginning with English common law and cementing itself over the history of our nation” that grand jury proceedings should remain secret. [Doc. 75 at 11]. This presumption, it argues, cuts against the requested invasion into the grand jury proceedings “based merely on disagreements over the facts of a case or assertions that the law is complicated.” [*Id.* at 1]. Furthermore, it continues, because Mr. Singla “provides nothing to support his accusations that the grand jury misunderstood or was misled as to the law and facts,” disclosure is unwarranted. [*Id.* at 8].

The Government’s position is well-taken. As this Circuit has held, “the party seeking disclosure of grand jury material must show a compelling and particularized need for disclosure.” (emphasis added). *Aisenberg*, 358 F.3d 1327, 1348 (11th Cir. 2004); See Also, *United States v. Procter & Gamble Co.*, 356 U.S. 677, 682 (1958)(stating that the “‘indispensable secrecy of grand jury proceedings' must not be broken except where there is a compelling necessity,” and that instances where the need outweighs the countervailing policy must “be shown with particularity.”). (internal citation omitted). Mr. Singla’s unsubstantiated allegations of impropriety concerning the nature of the evidence and the instructions presented to the grand jury fail to overcome the presumption of secrecy. These allegations also fail to establish a compelling need for disclosure. Accordingly, his requests for *in camera*




review of the above listed materials and disclosure of the grand jury's instructions are **DENIED**.

### **CONCLUSION**

Based on the foregoing reasons, the undersigned **RECOMMENDS** that Defendant's Renewed Motion to Dismiss Indictment (Counts One – Seventeen) for Lack of Specificity, [Doc. 68], be **GRANTED**; **RECOMMENDS** that Defendant's Renewed Motion to Dismiss Count Eighteen as Unconstitutionally Vague, [Doc. 69], be **DENIED IN PART/DEFERRED IN PART**; Defendant's Renewed Motion for Early Issuance of Rule 17(c) Subpoena, [Doc. 67], is **DENIED**; Defendant's Renewed Motion for Bill of Particulars, [Doc. 71], is **DENIED**; and Defendant's Renewed Motion to Compel Disclosure of Grand Jury Transcripts, [Doc. 70], is **DENIED**.

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

IT IS SO RECOMMENDED on this 17<sup>th</sup> day of July, 2023.

  
REGINA D. CANNON  
United States Magistrate Judge