

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

United States of America,

v.

Case No. 1:21-cr-228-MLB

Vikas Singla,

Defendant.

_____ /

OPINION & ORDER

Defendant, for the second time, asks the Court in two separate motions to dismiss an indictment the United States obtained against him charging him with various computer crimes. (Dkts. 68; 69.) He also filed a host of other motions. (Dkts. 67, 70, 71.) Magistrate Judge Regina D. Cannon issued an Order and Final Report and Recommendation (R&R), saying the Court should grant his motion to dismiss Counts One through Seventeen of his indictment, deny in part and defer in part his motion to dismiss Count Eighteen, and deny the remaining motions. (Dkt. 90). Both parties object to different portions of the R&R. (Dkts. 95; 96.) The Court adopts the R&R as modified herein, sustains the United States's

objections, overrules Defendant's objections, and denies Defendant's motions.

I. Background

The United States obtained an indictment against Defendant, charging him with eighteen violations of the Computer Fraud and Abuse Act of 1986 (CFAA). (Dkt. 1.) The charges involve his alleged attack on computers at the Duluth and Lawrenceville campuses of the Gwinnett Medical Center. (*Id.*) Count One alleges that “[o]n or about September 27, 2018,” Defendant “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.” (Dkt. 1 ¶ 3.) Counts Two through Seventeen allege that “[o]n or about September 27, 2018,” Defendant “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” several printers listed in a table and identified by brand, model, internal identification number, and IP address. (Dkt. 1 ¶ 5.) Count Eighteen alleges that “[o]n or about September 27, 2018,” Defendant “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 D2 Digitizer used by Gwinnett Medical Center in the Lawrenceville, Georgia hospital.” (Dkt. 1 ¶ 6.)

Defendant previously moved to dismiss the indictment, arguing the language of the charges lacks the specificity required by the Sixth Amendment to the United States Constitution and the Federal Rules of Criminal Procedure. (Dkt. 29.) The Magistrate Judge agreed, concluding the indictment failed to identify adequately the computers Defendant allegedly attacked or how he was not authorized to access one of those computers. (Dkt. 51.) The Court rejected the R&R, concluding the Magistrate Judge failed to consider the descriptive language of the indictment, and that all of the counts (1) sufficiently identified the

protected computers at issue, and (2) sufficiently pled Defendant exceeded (or attempted to exceed) his authorization in accessing the Hologic D2 Digitizer. (Dkt. 63.) The Court explained, however, that Defendant “raised a panoply of other arguments against the indictment” during various hearings and post-hearing briefs that the Magistrate Judge did not consider. (Dkt. 63 at 10–16.) The Court also “raised another issue on its own—whether Counts One through Seventeen must more fully describe how Defendant Singla caused or tried to cause the transmission of a program, code or command to the computers at issue in each count,” given that question “was not part of the” R&R. (Dkt. 63 at 16.) The Court said, if Defendant “believes his lingering arguments have merit, he may pursue them in a separate avenue” before the Magistrate Judge. (Dkt. 63 at 17.)

Defendant then filed two renewed motion to dismiss the indictment, raising his new arguments. (Dkts. 68; 69.) He also filed a motion for a bill of particulars (Dkt. 71); the early issuance of a subpoena for records related to victim devices alleged in the indictment (Dkt. 67); and the disclosure of transcripts and other materials from the grand jury proceedings that resulted in the indictment (Dkt. 70). Magistrate Judge

Cannon issued an R&R advising the Court how to dispose of those motions (Dkt. 90), and both parties objected. (Dkts. 95; 96.)

II. Standard

28 U.S.C. § 636(b)(1) requires district courts to “make a de novo determination of those portions of [an R&R] to which objection is made.” Any such objection “must specifically identify the portions of the [R&R] to which objection is made and the specific basis for objection.” *McCullars v. Comm’r, Soc. Sec. Admin.*, 825 F. App’x 685, 694 (11th Cir. 2020)¹; see *United States v. Schultz*, 565 F.3d 1353, 1360 (11th Cir. 2009) (“[A] party that wishes to preserve its objection must clearly advise the district court and pinpoint the specific findings that the party disagrees with.”). “Frivolous, conclusive, or general objections need not be considered by the district court.” *Marsden v. Moore*, 847 F.2d 1536, 1548 (11th Cir. 1988).

“It does not appear that Congress intended to require district court

¹ The Court recognizes *McCullars* and other cases cited herein are unpublished and not binding. The Court cites them nevertheless as instructive. See *Searcy v. R.J. Reynolds Tobacco Co.*, 902 F.3d 1342, 1355 n.5 (11th Cir. 2018) (“Unpublished cases do not constitute binding authority and may be relied on only to the extent they are persuasive.”).

review of a magistrate’s factual or legal conclusions, under a de novo or any other standard, when neither party objects to those findings.” *Thomas v. Arn*, 474 U.S. 140, 150 (1985). And, in most cases, “[a] party failing to object to [an R&R] waives the right to challenge on appeal the district court’s order based on unobjected-to factual and legal conclusions.” *McGriff v. Comm’r, Soc. Sec. Admin.*, 654 F. App’x 469, 472 (11th Cir. 2016). Ultimately, whether or not objections are filed, a district court “may accept, reject, or modify, in whole or in part, the findings or recommendations made by the magistrate judge.” 28 U.S.C. § 636(b)(1).

III. Motions to Dismiss Indictment

Defendant filed two motions seeking to dismiss the charges in his indictment that—if both were granted—would result in complete dismissal of the indictment. (Dkts. 68; 69.) His first motion deals with Counts One through Seventeen. (Dkt. 68.) His second deals with Count Eighteen. (Dkt. 69.)

A. Motion to Dismiss Counts One Through Seventeen

Defendant says Counts One through Seventeen of the indictment are constitutionally deficient for three reasons: (1) Count One is impermissibly vague because it alleges Defendant damaged a phone

system comprised of hundreds of different protected computers rather than a single protected computer; (2) Counts One through Seventeen violate the Fifth Amendment because they each contain an enhancement improperly charging Defendant with damaging multiple protected computers in a single count rather than identify a unique, uncharged protected computer, which he claims is required by the statute; and (3) Counts One through Seventeen are impermissibly vague because they fail to identify the particular “program, information, code, or command” and the alleged “damaged” caused by its “transmissions.” (Dkt. 68.)

The Sixth Amendment guarantees that “[i]n all criminal prosecutions, the accused shall enjoy the right . . . to be informed of the nature and cause of the accusation.” Const. amend. VI. Rule 7 of the Federal Rules of Criminal Procedure seeks to ensure this by requiring that an indictment contain a “plain, concise, and definite written statement of the essential facts constituting the offense charged.” Fed. R. Crim. P. 7(c)(1). The Supreme Court has said, “an indictment is sufficient if it, first, contains the elements of the offense charged and fairly informs a defendant of the charge against which he [or she] must defend, and, second, enables him [or her] to plead an acquittal or conviction in bar of

future prosecutions for the same offense.” *Hamling v. United States*, 418 U.S. 87, 117 (1974); *see also United States v. Steele*, 178 F.3d 1230, 1233-34 (11th Cir. 1999) (holding indictment sufficient if it “(1) presents the essential elements of the charged offense, (2) notifies the accused of the charges to be defended against, and (3) enables the accused to rely upon a judgment under the indictment as a bar against double jeopardy for any subsequent prosecutions of the same offense”). So it may not always be enough for the United States simply to quote the statutory language if that language does not adequately inform the defendant of the accusation he or she must defend. In that case, the United States must also include “a statement of the facts and circumstances as will inform the accused of the specific offense, coming under the general description, with which he [or she] is charged.” *Hamling*, 124 U.S. at 117–118.

1. Identification of Computers in Count One

First, Defendant says Count One is unconstitutionally vague because, rather than identify “a particular computer or device that bears a unique serial number or identifier,” it describes the “protected computer” as the Ascom phone system, which consists of “a collection of numerous computers and devices.” (Dkt. 68 at 9–11.) Defendant argues

this means 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.” (Dkt. 68 at 10–11.) The Magistrate Judge concluded Defendant’s argument is foreclosed because the Court already decided Count One adequately defines the “protected computer” he allegedly damaged. (Dkt. 90 at 15–16.) Defendant objects, saying the CFAA requires that the United States charge him with a “single, specific device” rather than a “computer system.” (Dkt. 96 at 8.) According to Defendant, because Count One instead charges him with damaging a system of multiple computers, it “fails to ensure that the putative ‘protected computer’ that [Defendant] allegedly damaged in Count One is the same protected computer for which the grand jury found probable cause to charge [him], and it fails to ensure that such damage allegedly occurred in the manner in which the grand jury determined it did.” (Dkt. 96 at 11.) The Court disagrees.

The Court expressly held in its prior order that “Count One . . . identifies the specific computer or *computers* Defendant Singla is alleged to have damaged or tried to have damaged,” and “[i]t tells him the day on

which he was alleged to have done that.” (Dkt. 63 at 6–7 (emphasis added).) Accordingly, it concluded Defendant “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.” (Dkt. 63 at 7 (emphasis added).) Nothing has changed.

Defendant contends the Magistrate Judge erred because it did not consider his new “statutory argument,” in which he claims the CFAA required the United States to “plead a single, specific victim computer to satisfy the Constitution.” (Dkt. 96 at 13.) The CFAA defines “computer” as a “high speed data processing device,” and a “protected computer” as, among other things, “a computer . . . which is used in or affecting interstate or foreign commerce or communication.” 18 U.S.C. §§ 1030(e)(1)–(e)(2). According to Defendant, because the statute defines a protected computer as a singular “computer” rather than the plural “computers,” the CFAA allows the United States to charge in a single count only harm to one computer “and not a group, network, or system of computers.” (Dkt. 96 at 9.) Regardless of whether the Magistrate Judge considered (or should have considered) that argument, it fails.

The United States Code sets a default rule of statutory construction that Congress’s use of the singular in a statute includes the plural. 1 U.S.C. § 1 (“In determining the meaning of any Act of Congress, unless the context indicates otherwise—words importing the singular include and apply to several persons, parties, or things[.]”). Nothing in the CFAA suggests Congress intended to foreclose the use of the plural when defining “computer” and “protected computer.” Indeed, reading the CFAA in context, it is clear that the statute specifically contemplates charging a defendant with damaging multiple protected computers. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(VI) (providing for higher sentence where defendant damages “10 or more protected computers”). It does not say those computers must be charged in different counts. Defendant concedes he can identify no case supporting his interpretation to the contrary. (Dkt. 68 at 9 n.4.) And the way other courts in this circuit have interpreted “protected computer” confirm Defendant’s reading is wrong. *See, e.g., Lighthouse List Co., LLC v. Cross Hatch Ventures Co.*, 2013 WL 11977916, at *6 (S.D. Fla. Aug. 9, 2013) (computers, computer systems, and databases constituted “protected computers”); *Continental Grp., Inc. v. KW Prop. Mgmt., LLC*, 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009)

(company’s “computer system” comprised “protected computers” under the CFAA).²

At bottom, Defendant’s beef with Count One is grounded in the same alleged pleading error as before: that the language in Count One fails to adequately identify the specific “protected computer” he allegedly damaged and that this ambiguity prevents him from raising due process claims. But as the Court explained in its prior order, a plain reading of the indictment adequately informs Defendant that on a particular day—September 27, 2018—Defendant damaged or tried to damage one *or more* computers that control the Ascom phone system at the Duluth hospital campus. (Dkt. 63 at 6.) “Following the resolution of this case, the indictment allows him to plead double jeopardy to bar any subsequent allegation that, on or near that day, he sent a program or command to try to damage those *computers*.” (Dkt. 63 at 7 (emphasis added).) The Court overrules Defendant’s objections to the Magistrate Judge’s findings on

² Although *Lighthouse List Co.* and *Continental Group, Inc.* are civil cases, they dealt with the same provisions of the CFAA defining its terms. Accordingly, the definition of “protected computer” is the same.

this issue.³

2. Felony-Loss Enhancement

Defendant next says the indictment is constitutionally infirm because the United States failed to identify at least one, unique “protected computer” in the felony-loss provision of 18 U.S.C. § 1030(c)(3)(I). (Dkt. 68 at 11.) He claims the statute requires both proof of loss to at least one person *and* loss affecting at least one other “protected computer” other than the charged computers. (*Id.*) According to Defendant, because the indictment requires the United States to prove only one of those predicates to justify application of the felony-loss enhancement, he risks being punished twice for “damage” caused to only

³ To the extent Defendant claims the indictment presents a variance issue (namely, that the grand jury might have had a different computer—or computers—in mind when it found probable cause to indict him), the Supreme Court has explained that courts are not to engage in such guesswork. *See Kaley v. United States*, 571 U.S. 320, 328 (2014) (“[A]n indictment ‘fair upon its face,’ and returned by a ‘properly constituted grand jury,’ we have explained, ‘conclusively determines the existence of probable cause’ to believe the defendant perpetrated the offense alleged.”) (citation and internal quotation marks omitted). Like the Magistrate Judge explained, if Defendant believes the evidence at trial varies from the charges in the indictment, he can raise this issue at the close of trial. *See United States v. Holt*, 777 F.3d 1234, 1261 (11th Cir. 2015) (improper “variance occurs when the facts *proved at trial* deviate from the facts contained in the indictment”) (emphasis added).

one “protected computer.” (Dkt. 68 at 12.) He also says a merger problem could arise if the United States relies on the same facts to support the underlying violation and the enhancement. (*Id.*) The Magistrate Judge disagreed, concluding the plain language of the statute shows “the applicable loss amount can be based on an aggregation of the loss caused by a defendant’s entire course of conduct,” and that any merger problems can be addressed after trial. (Dkt. 90 at 18–19.) Defendant objects, saying the Magistrate Judge misunderstood his argument, that the authority referenced in the R&R is inapposite, and that waiting to fix the problem until after trial would “be tantamount to illegally amending the [i]ndictment.” (Dkt. 96 at 20–27.) This Court disagrees.

The felony-loss enhancement triggers felony liability if the charged offense caused, or would have caused if completed:

[L]oss 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). The provision broadly defines “loss” 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 interruption of service.” 18 U.S.C. § 1030(e)(1). “[T]he statute requires only a total loss amount of \$5,000, which can be aggregated based on the conduct charged along with any relevant course of conduct during a 1-year period.” *Lanam v. United States*, 554 F. App’x 413, 417 (6th Cir. 2014); see Eleventh Circuit Pattern Jury Instructions, Criminal, Offense Instruction 42.3 (2020) (explaining felony-loss enhancement as “the damage result[ing] in [losses of more than \$5,000 during a one-year period [beginning [date], and ending [date]]”).

By its plain terms, the statute allows the United States to aggregate the loss caused by a defendant’s entire course of conduct in reaching the amount required to trigger felony liability. See *Merritt v. Dillard Paper Co.*, 120 F.3d 1181, 1185 (11th Cir. 1997) (“In construing a statute [the court] must begin, and often should end as well, with the language of the statute itself.”). As correctly noted by the Magistrate Judge, the felony-loss provision specifically identifies the potential harm a defendant could cause to multiple “protected computers” during an extended criminal episode. (Dkt. 90 at 19.) Consistent with this provision, the indictment

alleges Defendant's course of conduct against protected computers (either the charged protected computers or from related, other protected computers) caused an aggregate loss of at least \$5,000. (Dkt. 1 ¶¶ 3, 5 (alleging damage Defendant caused to the charged protected computers "caused and would, if completed, have caused . . . loss to Gwinnett Medical Center during the one-year period from [Defendant's] course of conduct affecting protected computers aggregating at least \$5,000 in value[.]").)

In arguing otherwise, Defendant says *Lanam* and the Eleventh Circuit's Pattern Jury Instructions do not support the Court's interpretation because (1) *Lanam* "does not even address the issue raised by [Defendant], and merely stands for the unremarkable proposition that the loss amount can be aggregated over several computers to satisfy the \$5,000 threshold," and (2) pattern jury instructions are not binding or precedential. (Dkt. 96 at 21.) Defendant is right, but he misses the point. While *Lanam* did not explicitly address whether the United States must allege a separate and unique protected computer to charge the felony-loss enhancement, it makes clear what is plain from the language of the statute: "the statute requires only a total loss amount \$5,000, which can

be aggregated based on the conduct charged *along with any relevant course of conduct during a 1-year period.*” 554 F. App’x at 417 (emphasis added). The pattern jury instruction merely confirms that plain reading. *See United States v. Adkinson*, 392 F. Supp. 2d 1378, 1381 (M.D. Ga. 2005) (“The Pattern Jury Instructions are not binding, even though the Court generally considers them a valuable resource, reflecting the collective research of a panel of distinguished judges.”).

Finally, Defendant takes issue with the Magistrate Judge’s conclusion that “any merger problem” related to the felony-loss enhancement “can be timely raised following trial or on appellate review.” (Dkt. 90 at 19.) Defendant says this “would require the Court to improperly add, by special verdict form and instructions, elements and facts not alleged in the Indictment and found by the grand jury concerning the identity of the computer upon which each felony-loss enhancement is predicated and any alleged loss associated with it.” (Dkt. 96 at 18–19.) According to Defendant, the Court cannot take a “wait and see approach” to this issue because the same “computers” on which Counts One through Seventeen are predicated may be the same ones used by the grand jury to potentially subject Defendant to the felony-loss

enhancement, thereby punishing him twice for the same conduct. (Dkt. 96 at 23.) Defendant’s argument, however, is based on the same misreading of the provision the Court already discussed. If ultimately (but doubtfully) this raises a merger issue, the Court can address it then.

3. “Program, Information, Code, or Command” and “Damage”

Finally, Defendant says Counts One through Seventeen must be dismissed because the United States failed to identify the particular “program, information, code, or command” Defendant allegedly transmitted and the “damage” it purportedly caused. (Dkt. 68 at 13.) He says “[a]t a minimum” the “indictment should allege . . . a particular transmission, program, code, or command . . . such as a particular malware, ransomware, or delete command” and “how each putative victim protected computer was damaged, such as by disabling or overwhelming a computer server or program, or corrupting or destroying a file or data.” (*Id.*) The Magistrate Judge agreed, concluding the indictment is too unspecific to “inform [Defendant] of the nature of the offenses he allegedly committed, rendering [it] unconstitutionally vague.” (Dkt. 90 at 25.) The United States objects, saying the Magistrate Judge “misunderstands the notice pleading requirements for an indictment”

and improperly required it to “allege detailed facts for each element of [the] offense conduct.” (Dkt. 95 at 7–8.)

The Court determines the sufficiency of an indictment from its face. *United States v. Salman*, 378 F.3d 1266, 1268 (11th Cir. 2004). “[C]ourts give the indictment a common sense construction, and its validity is to be determined by practical, not technical, considerations.” *United States v. Poirier*, 321 F.3d 1024, 1029 (11th Cir. 2003) (citation and internal quotation marks omitted). While an indictment must contain a statement of facts and circumstances sufficient to inform the accused of the specific offense with which he or she is charged, it need not lay out every detail of the case. *United States v. Sharpe*, 438 F.3d 1257, 1263 n.3 (11th Cir. 2006) (“It is not necessary for an indictment . . . to allege in detail the factual proof that will be relied upon to support the charges.”). “Ordinarily, ‘an indictment need do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime.’” *United States v. Jenkins*, 2022 WL 474704, at *3 (11th Cir. Feb. 16, 2022) (quoting *United States v. Stavroulakis*, 952 F.3d 686, 693 (11th Cir. 1992)). “[T]he appropriate test . . . is not whether the indictment might have been drafted with more clarity, but whether

it conforms to minimal constitutional standards.” *Poirier*, 321 F.3d at 1029 (quoting *United States v. Varkonyi*, 645 F.2d 453, 456 (5th Cir. 1981)).

In finding the indictment fatally nonspecific, the Magistrate Judge compared it to indictments in three other cases that contained more specific information about the kind of “program, information, code, or command” the defendant allegedly transmitted. (Dkt. 90 at 23–24.) But just because those indictments contained more detailed information does not automatically render the indictment here infirm. While the Magistrate Judge (and Defendant) might think the indictment could contain more specific factual allegations, the only question before the Court is whether the indictment sufficiently puts Defendant on notice about the criminal conduct with which the United States has charged him. The indictment charges that on a specific date (September 27, 2018), Defendant engaged in conduct (transmitting a program, information, code, or command) causing damage to specific protected computers at specific hospitals run by Gwinnett Medical Center. He cites nothing saying the CFAA’s terms are so vague they require more specificity. They are not.

A “program, information, code, or command” is something that can be sent to a computer to make it do something.⁴ By tracking the statutory language, the allegations in Counts One through Seventeen thus plainly charge Defendant with sending instructions to specific computers on specific days to damage the computers. That is enough to put him on notice. *See United States v. Middleton*, 35 F. Supp. 2d 1189, 1191 (N.D. Cal. 1999) (indictment charging that defendant “knowingly transmitted code and commands to a computer system” was sufficient because “[t]he acts with which defendant is alleged to have done are certainly set forth with adequate particularity, tracking the language of the statute”). No authority suggests the United States must identify in the indictment the

⁴*See Program*, MERRIAM-WEBSTER ONLINE DICTIONARY, <https://www.merriam-webster.com/dictionary/program> (last visited Sept. 6, 2023) (“[A] sequence of coded instructions that can be inserted into a mechanism (such as a computer)[.]”); *Information*, MERRIAM-WEBSTER ONLINE DICTIONARY, <https://www.merriam-webster.com/dictionary/information> (last visited Sept. 6, 2023) (“[A] signal or character (as in a communication system or computer) representing data[.]”); *Code*, MERRIAM-WEBSTER ONLINE DICTIONARY, <https://www.merriam-webster.com/dictionary/code> (last visited Sept. 6, 2023) (“[I]nstructions for a computer (as within a piece of software)[.]”); *Command*, MERRIAM-WEBSTER ONLINE DICTIONARY, <https://www.merriam-webster.com/dictionary/command> (last visited Sept. 6, 2023) (“[A] line of code [] instructing a computer to send such a signal[.]”).

name of the code or instruction Defendant allegedly sent. The Court will not impose that requirement.

But, the indictment is even more specific because it alleges exactly what the “program, information, code or command” Defendant transmitted did (or attempted to do)—damaged the computers. There is nothing vague or unclear about the “damage” Defendant is alleged to have caused. The CFAA expressly and broadly defines “damage” as “any impairment to the integrity or availability of data, a program, a system, or information.” 18 U.S.C. § 1030(a)(5)(A).

Putting all of that together shows the sufficiency of the United States’s allegations. For Count One, the United States alleges that, on a specific date, Defendant sent instructions to the computers that operate the Ascom phone system at the Duluth hospital and thus impaired (or attempted to impair) the integrity or availability of the Ascom phone system; and for Counts Two through Seventeen it alleges Defendant sent instructions to the computers identified in those counts and by doing that impaired (or attempted to impair) the integrity or availability of each of the listed printers. It took the United States one sentence to explain this allegation for Count One at a prior hearing: “the way that the defendant

damaged the Ascom Phone System was he sent a configuration . . . file to the server that was then pushed out onto all the handsets that rendered all the handsets offline and shut down the network.” (Dkt. 62 at 18:10–14.) Similarly, the United States points to discovery showing Defendant’s alleged attack rendered the printers unusable. (Dkt. 77 at 19.) Although this extraneous evidence does not supplement the indictment, it does show the indictment properly charges the thing Defendant is alleged to have transmitted and the “damage” Defendant is alleged to have caused. *United States v. Roque*, 2013 WL 2474686, at *5 (D.N.J. June 6, 2013) (“The statutory definition of ‘damage’ may be very inclusive, but it is not unclear.”)

In holding otherwise, the Magistrate Judge relied on *Russell v. United States* and related cases, saying they show the indictment must contain more than the date and statutory descriptions of the charged offense. (Dkt. 90 at 21–22 (citing 369 U.S. 749 (1962).) First, courts—including the Supreme Court—have made clear that *Russell* deviates from generally applicable principles for indictments given the nature of the charges in that case. *See United States v. Resendiz-Ponce*, 549 U.S. 102, 110 (2007) (noting charges brought under statute at issue in *Russell*

have a “special need for particularity”); *United States v. Stringer*, 730 F.3d 120, 125–26 (2d Cir. 2013) (“[I]t is clear that the Supreme Court’s decision in *Russell* must be seen as addressed to the special nature of a charge of a refusal to answer questions in a congressional inquiry and not as a broad requirement applicable to all criminal charges that the indictment specify how each essential element is met.”). *Russell* does, however, properly stand for the proposition that detailed factual specificity is required in an indictment only where a more general allegation does not satisfy an element of the charged offense. *See United States v. Huggans*, 650 F.3d 1210, 1219 (8th Cir. 2011) (noting specificity over certain questions defendants allegedly refused to answer was necessary in *Russell* because the statute “did not criminalize refusal to answer non-pertinent questions”). The CFAA is totally different. Its statutory language contains no confusion as to the nature of the offense elements, nor does it require specificity to avoid the potential criminalization of non-criminal conduct. *Russell* is useless in answering the questions at issue here.⁵

⁵ The other two cases relied upon by the Magistrate Judge similarly provide no help. *United States v. Peterson* involved the same issue as *Russell*, where the charging language did not clearly allege an element of

When read in context, contrary to the Magistrate Judge’s conclusion, the indictment does not merely provide “generic terms” that must “descend to particulars” to adequately notify Defendant about the charges. (Dkt. 90 at 25.) The allegations in Counts One through Seventeen charge Defendant with—on a particular day—knowingly causing the transmission of a program, code, or command to intentionally cause damage to the Ascom phone system and to a list of individual printers. The indictment does not tell Defendant to look to all the computer commands in the world, all the commands at Gwinnett Medical Center, or even all the commands sent to the protected computers. Rather, the indictment closely constrains to the text of the charges the set of possible codes and commands and the damage they allegedly caused to specific computers on or about September 27, 2018. Defendant’s motion to dismiss Counts One through Seventeen fails.

the offense. *See* 544 F. Supp. 2d 1363, 1375 (M.D. Ga. 2008). And in *United States v. Tripodis*, a fraud indictment failed to specify who exactly had been defrauded or of what they had been defrauded—two elements of the charged offenses—even though the United States’s filings suggested multiple possibilities. 2020 WL 914681, at *3. The indictment here has neither of these problems.

B. Motion to Dismiss Count Eighteen

In a separate motion, Defendant asks the Court to dismiss Count Eighteen on the ground that the provision of the CFAA it charges—18 U.S.C. § 1030(a)(2)(C)—is unconstitutionally vague. (Dkt. 69.) The Magistrate Judge concluded the provision is not vague on its face because Defendant did not meet his burden of showing “that no set of circumstances exist under which the [provision] would be valid.” (Dkt. 90 at 27.) Defendant objects, saying § 1030(a)(2)(C) is unconstitutionally vague because “it purports to criminalize every use of a protected computer of any person without permission even if the user has no idea that such permission is needed.” (Dkt. 96 at 28–29.) The Court disagrees with Defendant.

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). Criminal statutes must define an 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.” *United States v. Fisher*, 289 F.3d 1329, 1333 (11th Cir. 2002) (citation omitted). “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). A facial challenge requires the defendant to show “no set of circumstances under which the [statute] would be valid, or that the statute lacks any plainly legitimate sweep.” *United States v. Stevens*, 559 U.S. 460, 472 (2010) (citations and internal quotation marks omitted); *see also SisterSong Women of Color Reproductive Justice Collective v. Governor of Ga.*, 40 F.4th 1320, 1327 (11th Cir. 2022). Importantly, however, a criminal defendant “who engages in some conduct that is clearly proscribed [by the statute] cannot complain of the vagueness of the law as applied to the conduct of others.” *Stardust, 3007 LLC v. City of Brookhaven*, 899 F.3d 1164, 1176 (11th Cir. 2018); *see also Kashem v. Barr*, 941 F.3d 358, 375 (9th Cir. 2019) (“[A] defendant who cannot sustain an as-applied vagueness challenge to a statute cannot be the one to make a facial vagueness challenge to a statute.”).

18 U.S.C. § 1030(a)(2)(C) prohibits a person from, among other things, “intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer.” Defendant emphasizes that applying the

“without authorization” or the “exceeds authorization access” elements involves “a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within a system.” (Dkt. 69 at 3 (quoting *Van Buren v. United States*, 141 S. Ct. 1648, 1658–59 (2021).) According to Defendant, “nothing in the statute gives fair notice to the computer user or sufficient guidance to federal prosecutors and agents enforcing the statute as to when such gates are ‘up-or-down,’” authorizing criminal prosecution against potentially innocent users who “wander[] into an unprotected area of a computer that does not belong to him [or her].” (Dkt. 69 at 4.) But Defendant’s argument that there may be some hypothetical cases where § 1030(a)(2)(C) is harder to apply does not mean the provision is unconstitutionally vague *as applied to him or her*. The indictment properly alleges Defendant committed acts that § 1030(a)(2)(C) clearly makes criminal—that is, that he intentionally accessed without authorization (or exceeded any authorized access to) the Hologic R2 Digitizer and obtained information from that computer. Defendant cannot feign he did not know his level of authorization to access that computer because—as discussed in more detail below—he had no

business with the hospital or any right whatsoever to access the computer. Defendant cannot raise a facial vagueness challenge to § 1030(a)(2)(C).

In arguing otherwise, Defendant says the Supreme Court has recently held that an otherwise impermissibly vague provision is not rendered constitutional “merely because there is some conduct that clearly falls within the provision’s grasp.” (Dkt. 96 at 29 (quoting *Johnson v. United States*, 576 U.S. 591, 602 (2015).)⁶ But regardless of whether *Johnson* overruled the “vague-in-all-its-applications standard,” it did “not jettison the [] rule” “prohibiting defendants whose conduct a

⁶ In holding Defendant had not met his burden to show § 1030(a)(2)(C) vague on its face, the Magistrate Judge relied only on the standard from *Stevens* that a statute is not facially vague if it can be applied constitutionally in even a single case. It appears *Johnson* did away with that standard. *See* 576 U.S. at 602 (“[A]lthough statements in some of our opinions could be read to suggest otherwise, our *holdings* squarely contradict the theory that a vague provision is constitutional merely because there is some conduct that clearly falls within the provision’s grasp.”) (emphasis in original). After *Johnson*, however, the Eleventh Circuit has still relied on that standard in concluding certain statutes are not impermissibly vague. *See, e.g., United States v. Gruezo*, 66 F.4th 1284, 1293 (11th Cir. 2023); *SisterSong*, 40 F.4th at 1327. If that standard is still good law, the Magistrate Judge was right in finding Defendant’s facial challenge fails because he did not show there is no set of circumstances under which § 1030(a)(2)(C) would be valid. But even if it is not, Defendant’s argument fails for the reasons discussed above.

statute clearly proscribes from bringing vagueness challenges.” *United States v. Hasson*, 26 F.4th 610, 619 (4th Cir. 2022). Defendant’s facial challenge still fails.

IV. Motion for Bill of Particulars

Defendant moves in the alternative for a bill of particulars, saying the indictment “fails to provide facts sufficient to enable [him] to prepare his defense and avoid the possibility of prejudicial surprise at trial.” (Dkt. 71 at 1.) The Magistrate Judge concluded that, because the United States already provided Defendant with all the information he seeks, “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.” (Dkt. 90 at 36.) Defendant objects, arguing that the United States did not provide adequate information in response to each piece of information he seeks. (Dkt. 96 at 30–37.)

Rule 7 of the Federal Rules of Criminal Procedure allows a court to direct the United States 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 (11th Cir. 1985). “A request for a 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.” *Id.* “[G]eneralized discovery”, however, “is not the proper function of a bill of particulars.” *Id.* 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 (11th Cir. 1986). Nor can a bill of particulars “be used as a weapon to force the government into divulging its prosecution strategy.” *United States v. Burgin*, 621 F.2d 1352, 1359 (5th Cir. 1980). For these reasons, a bill or particulars is also not a vehicle by which a defendant can force the United States to answer all of his or her questions about the United States’s case, its evidence, or its theories of prosecution.

A. Protected Computer

Defendant requests identification of the particular “protected

computer” described in Count One. (Dkt. 71 at 9.) The Magistrate Judge concluded the United States “already identified (and [this Court] affirmed) the ‘protected computer’ as to computer or computers that operate the Duluth hospital’s Ascom phone system.” (Dkt. 90 at 34.) Defendant says this was error because—like he argued in his motion to dismiss Count One—“a ‘system’ is not the same thing as a ‘computer’ under the CFAA, and the [United States] has only identified the former and not the latter.” (Dkt. 96 at 31.) Defendant’s argument fails for the same reasons the Court described above and in its prior order.

Defendant also requests identification of the “other” protected computer that supports the felony-loss enhancement in Counts One through Seventeen. (Dkt. 96 at 31.) It appears the Magistrate Judge did not address this argument. Regardless, it fails because—as the Court already concluded—the United States did not have to identify a separate, unique protected computer for the felony-loss enhancement to apply. The United States properly alleged Defendant caused loss to Gwinnett Medical Center of at least \$5,000 in value (during the one-year period) from his course of conduct effecting the protected computers. (Dkt. 1 ¶¶ 3, 5.)

Finally, Defendant points out that the Court ruled the indictment “adequately alleges the identity of the protected computer” in Count Eighteen (a Hologic R2 Digitizer), but says “neither the [i]ndictment nor the discovery seems to identify which computer [Defendant] is alleged to have access without authorization, and whether that computer is a different computer from the protected computer.” (Dkt. 71 at 14–15.) Defendant seems to be looking for a problem where there is none or perhaps refusing to comprehend the simple language of the charge. Count Eighteen identifies only one computer “that is, a Hologic R2 Digitizer used by Gwinnett Medical Center in the Lawrenceville, Georgia hospital.” (Dkt. 1 ¶D 7.) Clearly, the United States alleges it is the computer Defendant accessed without authorization and the protected computer. There can be no other conclusion. Defendant, conceding the obvious, declares the United States has “clarified in its briefing below that the computer that [Defendant] allegedly accessed and the computer from which he allegedly obtained information are the same computer”—that is, the Hologic R2 Digitizer. (Dkt. 96 at 31.) He says “[a]s a result, the [United States] would suffer no prejudice from committing to this information in a bill of particulars.” (*Id.*) But that is not the test, nor is

it the point of a bill of particulars. Defendant clearly does not need this information in a bill of particulars to adequately prepare a defense because *he concedes he has that information*.

B. Interstate Commerce

Next, Defendant says the indictment does not allow him to evaluate why or how any charged protected computer is alleged to have been “‘used in or affecting interstate or foreign commerce or communication’ at the time of the alleged offense.” (Dkt. 71 at 10 (quoting 18 U.S.C. § 1030(e)(2)(B)).) Specifically, he argues as to Count One that, even though the United States provided him discovery showing the Ascom phone system was connected to the internet at the time of the offense, it improperly “speaks in terms of the entire system” rather than “the specific device at issue.” (Dkt. 71 at 11.) As the Magistrate Judge concluded, that argument fails for the same reasons as before.

As to Counts Two through Seventeen, it appears the Magistrate Judge did not expressly address Defendant’s contention that “[n]either the [i]ndictment nor the discovery appears to provide information sufficient to evaluate why or how each of the [Gwinnett Medical Center] printers . . . were used in or affecting interstate commerce at the time of

the offense.” (Dkt. 71 at 13.) He says he “has been unable to locate any logs or network infrastructure information in the discovery illustrating internet connectivity as to the printers, and no discovery on [Gwinnett Medical Center’s] engagement in interstate commerce appears to have been provided.” (*Id.*) Similarly, as to Count Eighteen, he says he has no discovery showing that the Hologic R2 Digitizer is connected to the internet or somehow used in interstate commerce. (Dkt. 71 at 15–16.)

Defendant’s argument on this front fails for two reasons. As a threshold matter, the indictment alleges that the computers at issue in each count were “protected computers,” which is defined to mean, among other things, a computer “used in or affecting interstate or foreign commerce.” *See* 18 U.S.C. § 1030(e)(2)(B). Defendant cites no authority to suggest the United States must explain in any detail how the computers impacted interstate commerce. Given the importance of an interstate nexus in many federal crimes (including Hobbs Act charges, firearm offense, carjacking crimes, wire and mail fraud charges, child exploitation crimes, bank fraud crimes, and so many more) it would be strange if the United States had to allege details of the connection to interstate commerce in every instance. The United States has alleged

the computers were used in or affected interstate commerce and will have to prove that. That Defendant explains ways in which the United States could prove the interstate commerce component shows he understands how to prepare a defense to that element. (Dkt. 71 at 10–11, 15–16 (explaining computers—including those alleged in Counts Two through Eighteen—would qualify if they were connected to the internet or “somehow used in interstate commerce by virtue of the healthcare business”).) While he may not yet have located “logs or network infrastructure information in the discovery illustrating internet connectivity,” information about “[Gwinnett Medical Center’s] engagement in interstate commerce,” or documents showing “how the Hologic R2 Digitizer is connected to the internet or somehow used in interstate commerce” he clearly understands the United States’s burden of showing such connectivity. Of course, if the United States has not timely produced such records it will not be permitted to introduce them at trial.

C. Damage

Defendant next requests specificity as to the “damage” element for

Counts Two through Seventeen. (Dkt. 71 at 13–14.)⁷ Specifically, he says “neither the [i]ndictment nor the discovery appears to contain information about how or the extent to which any [Gwinnett Medical Center] printer is alleged to have been damaged as a result of the incident.” (Dkt. 71 at 13.) But, as the Magistrate Judge explained, the United States pointed to discovery identifying the damage Defendant allegedly caused when he attacked the network printers: “the attack on the network printers caused patient health information and the threatening message ‘WE OWN YOU!’ to be printed from the network printers.” (Dkt. 77 at 19.) Defendant says this does not “shed any light on whether or how this allegedly resulted in ‘impairment to the integrity or availability of data, a program, a system, or information’ as required by the CFAA.” (Dkt. 96 at 33 (quoting 18 U.S.C. § 1030(e)(8).) But Defendant then goes on to list a number of ways the United States might

⁷ Defendant says in his objections that he also requests a bill of particulars as to the damage element in Count One. (Dkt. 96 at 29.) He did not make such a request in his motion. And—contrary to his assertion—the Magistrate Judge did not address it in the R&R. In any event, his only argument as to Count One is the same as before—namely, that the United States improperly identifies a system rather than a particular computer. This argument fails for the reasons states.

prove Defendant's alleged attack impaired the printers, including by showing the printers were unavailable "while they were actually printing the alleged print jobs" or that the printers' data was impacted. (*Id.*) Defendant has clearly identified ways in which the United States could seek to prove this element of the offense. Although Defendant may prefer more detailed information regarding the United States's theory, he is not entitled to "detailed exposition of [the United States's] evidence" or "the legal theories upon which it intends to rely at trial." *United States v. Roberts*, 174 F. App'x 476, 477 (11th Cir. 2006) (citation omitted).

D. Loss

Defendant next contends he is entitled to more detailed information about the specific losses he is alleged to have caused in Counts One through Seventeen. (Dkt. 71 at 11–12, 14.) But, as he concedes, the United States gave him a summary "showing a total loss amount and line-items for categories such as legal fees, consulting fees, and lost employee time." (Dkt. 71 at 11.) It is unclear what more he wants. He complains this information is "merely generic, aggregate information untethered to any particular computer." (Dkt. 96 at 34.) But he points to no authority saying the United States must—in a bill of particulars—

itemize the losses it alleges Defendant caused or categorize it by each computer he allegedly damaged.

E. Medical Care Enhancement

Defendant also requests specific information about “any actual or potential impact of the alleged incident on patient care.” (Dkt. 71 at 12.) As the Magistrate Judge explained, the United States has provided discovery showing that the Ascom phone system was “critical . . . for the hospital and patient care.” (Dkt. 77 at 21.) Similarly, discovery describes how the alleged attack required that Defendant “pull[] for quarantine and review” its printers after they began printing patient health information and referenced certain print jobs as impacting patient care. (*Id.*) And—to state the obvious—common sense dictates that the devices owned and used by a hospital (including those used by staff members to communicate with one another) may have an actual or potential impact on patient care.

F. Unauthorized Access and Exceeding Authorized Access

Finally, Defendant says he needs specific information about “how or whether [Defendant’s] initial access was without authorization, how [Defendant] exceeded or attempted to exceed authorized access, what

notice [Gwinnett Medical Center] provided to inform [Defendant] that his alleged access was unauthorized or exceeded authorized access, and how or why he was not entitled to obtain the information that he allegedly obtained.” (Dkt. 71 at 15.) The Magistrate Judge concluded that Defendant “cannot feign surprise regarding his professional association with [Gwinnett Medical Center] or the boundaries of his access to its communication systems,” given that he was not an employee, did not have any business with Gwinnett Medical Center, and had no lawful reason to access Gwinnett Medical Center’s network or to obtain and publish patient information. (Dkt. 90 at 36.) Defendant contends the Magistrate Judge erred on this front because Gwinnett Medical Center “appears to have left its facility and its network open to the public at all hours of the day and night,” and the United States did not provide any information about authentication features or other barriers, warnings, or notices Defendant allegedly received, or contractual access limitations of which he was aware. (Dkt. 96 at 36.)

Defendant’s argument belies common sense. The Court already held the indictment did not have to explain the “professional relationship [Defendant] had (if any) with [Gwinnett Medical center], to what extent

he had access to [Gwinnett Medical Center’s] internal network, or to what degree he exceeded his authority while accessing [Gwinnett Medical Center’s] network.” (Dkt. 63 at 10–11.) It explained “[t]he term ‘authorization’ has a simple meaning,” and that “the United States is saying (as one alternative) that [Defendant] had no permission or approval to access the Hologic R2 Digitizer on September 27, 2018,” and that, to the extent he did, “he exceeded the scope of his permission by accessing information he had no right to access.” (Dkt. 63 at 11.) This puts Defendant “on notice of what he was alleged to have done.” (Dkt. 63 at 12.) That is all that is required.

V. Motion for Early Issuance of Rule 17(c) Subpoena

Defendant asks the Court for early issuance of a subpoena to seek four categories of documents: (1) firewall activity logs relating to any Gwinnett Medical Center computer or device alleged in the indictment during the alleged attack; (2) reports of any third-party breach response or breach remediation consultants on the causes of the alleged attack; (3) documents concerning any cybersecurity incidents at Gwinnett Medical Center prior to the alleged attack; and (4) detailed information regarding Gwinnett Medical Center’s breach response and remediation expenses.

(Dkt. 83.) He says, given the “highly technical nature” of the evidence in this case, he needs early disclosure to allow him to prepare his defense, enable his experts to examine the documents, and avoid delaying trial. (Dkt. 83 at 6.) For various reasons, the Magistrate Judge concluded he was not entitled to any of this information. (Dkt. 90 at 41–42.) Defendant objects. (Dkt. 96 at 37–48.)

Rule 17 of the Federal Rules of Criminal Procedure allows a court to issue a subpoena ordering a witness to produce information and documents “before trial or before they are to be offered in evidence.” Fed. R. Civ. P. 17(c)(1). To obtain early production, the party seeking the information 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). Rule 17 “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.” *United States v. Silverman*, 745 F.2d 1386, 1397 (11th Cir.

1984). It is “not intended to provide an additional means of discovery for any party in criminal cases.” *Id.* 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).

A. Firewall Activity Logs

Defendant says it needs “[f]irewall activity logs respecting any [Gwinnett Medical Center] computer or device alleged in the Indictment during the 2018 incident” because “it is standard operating procedure in every breach remediation investigation for them to be collected and revised and the logs contain information that will exculpate [Defendant].” (Dkt. 67 at 6.) Should those records not exist, Defendant says, Gwinnett Medical Center should be required to “formally confirm that it destroyed or failed to preserve them.” (Dkt. 67 at 7.) The Magistrate Judge concluded there “is no good faith basis for issuance of a subpoena for these records” because the United States “already informed [Defendant] that neither it nor [Gwinnett Medical Center] are in possession of these records.” (Dkt. 90 at 41.) Defendant argues the Magistrate Judge erred by allowing the United States “to stand in the

shoes of a non-party witness (here, [Gwinnett Medical Center]) in order to shield that witness from the obligation of conducting its own diligent search for relevant records, or even from providing some representation of its own that it has been unable to locate such records after conducting a diligent search.” (Dkt. 96 at 40.)

Defendant’s request for the firewall logs (which he cannot be sure even exist) or for Gwinnett Medical Center to confirm under oath that it does not have them is tantamount to asking for broad non-party discovery. Indeed, it is the exact sort of “fishing expedition” to “develop[] investigative leads” that is improper under Rule 17. Defendant cannot use Rule 17 to force the victim in this case to cobble together unspecified information that it may not even have or to produce an attestation as to its lack of documentation. *See United States v. Cory*, 2022 WL 997336, at * 4 (M.D. Fla. Apr. 1, 2022) (“[I]ssuing a subpoena under Rule 17(c) based on Defendant’s good faith belief and the *possibility* that materials exist is not enough.”) (emphasis in original). The Court adopts the Magistrate Judge’s determination Defendant is not entitled to the early issuance of Rule 17(c) subpoenas.

B. Third-Party Reports

Next, Defendant requests “[a]ny” breach reports from third-party experts or consultants on a broad range of topics. (Dkt. 67 at 7.) He says he needs these reports to ensure Defendant “is not being accused of causing damage or being held responsible for remediation costs that are actually due to other causes.” (*Id.*) The Magistrate Judge concluded Defendant’s request fails because it “is so broad that it fails to comport with the requirement that the subpoena target ‘specifically identified documents.’” (Dkt. 90 at 42 (citing *United States v. Arditti*, 955 F.2d 331, 346 (5th Cir. 1992).) Defendant argues the Magistrate Judge erred because “‘breach report’ is a term of art that is understood by information technology professionals . . . to be a single, specific document.” (Dkt. 96 at 42.)

Defendant’s request for any potential report of a third-party consultant or expert is plainly overbroad. Even if “breach report” is a term of art that might refer to a single document, Defendant’s request makes clear that he does not know if such a report even exists. That Defendant asks for “any” breach report and, in the alternative, for “notes, presentations or workpapers functioning as the equivalent of such

report” (Dkt. 67 at 7), makes clear that Defendant has no specific breach report in mind and attempts to improperly use Rule 17 “as a discovery device.” *Arditti*, 955 F.2d at 346 (citation omitted).

C. Prior Cybersecurity Incidents

Defendant also requests “[d]ocuments concerning any cybersecurity incidents at [Gwinnett Medical Center] prior to the 2018 incident.” (Dkt. 67 at 8.) He says it has been “publicly reported” that Gwinnett Medical Center has suffered cyberattacks in the past, but that the United States’s discovery “omits any information about any other cybersecurity incidents or issues at [Gwinnett Medical Center], ever.” (Dkt. 67 at 9 (emphasis omitted).) According to Defendant, without this information, he “has no way of testing whether the [United States] has mistakenly attributed the conduct of others to him, and whether it is employing overinclusive cost estimates that include remediation costs associated with prior, unrelated incidents.” (*Id.*) The Magistrate Judge concluded “this request lacks specificity and is of limited relevancy given [Defendant’s] mere assumption that [Gwinnett Medical Center] previously suffered the same harm alleged in the instant case.” (Dkt. 90 at 42.) Defendant argues his request is limited by the language of the proposed subpoena, which says

it seeks “[d]ocuments sufficient to show any cybersecurity incidents at [Gwinnett Medical Center] in the five year period prior to the 2018 incident,” that “cybersecurity incidents” is a term of art, and that the information is relevant to rebut the United States’s contention he is responsible for “all of [Gwinnett Medical Center’s] problems and remediation costs.” (Dkt. 96 at 44.)

Regardless of the limiting language in the proposed subpoena, Defendant again tries to use Rule 17 to improperly engage in discovery. Defendant’s request seeks information about incidents he does not even know have occurred.⁸ And even if they did, he does not know whether they were the same types of attacks the United States alleges he committed in this case. This request is just another example of Defendant’s attempts to use Rule 17 to go on an unwarranted fishing expedition. *See United States v. Cole*, 755 F.2d 748, 759 (11th Cir. 1985)

⁸ Defendant says “[i]t has been publicly reported that [Gwinnett Medical Center] experienced a debilitating malware attack in late 2011,” citing a news article. (Dkt. 67 at 9.) But he claims his proposed subpoena is not overbroad because it is limited to information about cybersecurity incidents that took place within five years before the alleged attack in 2018. So, the only specific cybersecurity incident he references took place outside the timeframe of the subpoena and cannot serve as the basis for any specific document he seeks.

(unsubstantiated allegations do not satisfy particularized need standard under Rule 17).

D. Breach Response Expenses

Finally, Defendant requests “[r]ecords of [Gwinnett Medical Center’s] reasonable attorneys’ fees, consultant fees, and other costs” related to responding to and remediating the alleged attack. (Dkts. 67 at 9; 67-1 at 3.) The Magistrate Judge concluded this request is “so broadly drafted that it fails to meet the specificity standard Rule 17 requires,” particularly because it not only seeks “detailed information” about Gwinnett Medical Center’s breach response, but also “receipts, invoices, billing narrative, payment records and related correspondence.” (Dkt. 90 at 43.) According to the Magistrate Judge, this “could arguably include attorney/client privileged materials, emails, and text messages.” (*Id.*) Defendant again argues the request is “cabined by the limiting language” in the proposed subpoena, that it “could conceivably be satisfied simply via production of the billing invoices for the short period during and after the 2018 attack” for third parties Gwinnett Medical Center engaged, and that attorney billing invoices are routinely produced in similar cases. (Dkt. 96 at 45–46.)

Defendant's request is overly broad for the same reasons as his other requests. Contrary to his argument, his request is in no way limited to the billing invoices he now claims it is. Like with all of his requests, this one is a "scattershot, dragnet attempt[] to discover evidence not presently known to exist." *United States v. Winner*, 2018 WL 1998311, at *2–3 (S.D. Ga. Apr. 27, 2018).

Defendant asks, in the alternative, for the Court to modify his proposed subpoena such that his requests are no longer overbroad. (Dkt. 96 at 48.) As it stands, those requests are so overbroad and inappropriate under Rule 17 that the Court cannot even see how it would do that. Nor does Defendant offer his own proposal. The Court assesses the appropriateness of Defendant's subpoena request based upon what he requested, not hypothetical limitations he includes as argument in attacking the Magistrate Judge's conclusion. It is not the Court's role or responsibility to pare down an overly broad and improper request to the proper scope. That is Defendant's role. His motion for early Rule 17(c) subpoenas fails in its entirety.

VI. Motion to Compel Disclosure of Grand Jury Transcripts

Defendant moves the Court to compel the disclosure of grand jury

transcripts because he believes the United States failed to properly instruct and advise the grand jurors as to the applicable law and facts regarding certain elements of the CFAA. (Dkt. 70 at 3.) The Magistrate Judge concluded Defendant’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” given to grand jury proceedings. (Dkt. 90 at 48.) Defendant objects, saying “the wildly incorrect legal positions adopted by the [United States] on several important statutory interpretation issues under the CFAA” and the indictment’s purported pleading errors warrant “ordering the [United States] to disclose its instructions and legal advice to the grand jury to determine if these critical errors . . . render [Defendant’s] indictment invalid and due to be dismissed.” (Dkt. 96 at 49.) Defendant is wrong.

“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.3d 1327, 1346 (11th Cir. 2004). To that end, Rule 6 of the Federal Rules of Criminal Procedure prohibits individuals involved in grand jury proceedings—

including the grand jurors themselves—from disclosing matters “occurring before the grand jury.” Fed. R. Crim. P. 6(e)(2)(B). Rule 6 also provides for certain exceptions under which a court may authorize disclosure of grand jury materials. Pertinent here, the court may disclose “a grand-jury matter . . . 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)(ii). A defendant attempting to rely on this exception must show “a compelling and particularized need for disclosure.” *Aisenberg*, 358 F.3d at 1348. A defendant’s “unsubstantiated allegations of grand jury manipulation do not satisfy the ‘particularized need’ standard.” *Cole*, 755 F.2d at 759. “Additionally, a blanket request for all grand jury materials cannot be described as the kind of particularized request for the production of otherwise secret information.” *Beiter v. United States*, 2023 WL 1980773, at *2 (11th Cir. Feb. 14, 2023) (citing *Aisenberg*, 358 F.3d at 1349).

Defendant asks for an extraordinary amount of secret information:

(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.

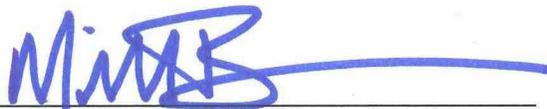
(Dkt. 70 at 8.) In essence, Defendant asks for “all grand jury materials.” It is hard to imagine what else he could ask for. So, his request certainly is not particularized. And even if it were, Defendant has not come close to showing a compelling need for the material. He offers only his contention that—based on its pre-trial briefing, legal arguments, and the indictment—the United States erroneously interpreted the CFAA, and therefore “must have” incorrectly instructed the grand jury regarding the elements of the offense. (Dkt. 70 at 1–2.) He offers nothing to support his theory that the grand jury was misinstructed. This is precisely the sort of unsubstantiated, purely speculative allegation that cannot support the very high bar for disclosure. Defendant is not entitled to any grand jury material.⁹

⁹ Defendant asks alternatively for the Court to examine the grand jury materials in camera to determine if the United States incorrectly instructed the grand jury. (Dkt. 96 at 51.) Given that Defendant does not even come close to meeting the standard required for disclosure, the Court concludes in camera review is not warranted.

VII. Conclusion

The Court **SUSTAINS** the United States's Objections (Dkt. 95), **OVERRULES** Defendant's Objections (Dkt. 96), and **ADOPTS IN PART** and **REJECTS IN PART** the Magistrate Judge's R&R (Dkt. 90). The Court **DENIES** Defendant's Motion for Early Issuance of Rule 17(c) Subpoena (Dkt. 67), Motion to Dismiss Indictment for Lack of Specificity (Dkt. 68), Motion to Dismiss Count 18 of the Indictment as Unconstitutionally Vague (Dkt. 69), Motion to Compel of Disclosure of Grand Jury Transcripts (Dkt. 70), and Motion for Bill of Particulars (Dkt. 71). The Court **SETS** a status conference for **September 19, 2023, at 10:00 a.m.**, to take place before the Honorable Michael L. Brown, in Courtroom 1906, Richard B. Russell Federal Building, 75 Ted Turner Drive, SW, Atlanta, Georgia 30303. The time between the date of this Order and the status conference shall be excluded in calculating the date on which the trial of this case must commence under the Speedy Trial Act. The Court finds that the delay is for good cause and the interests of justice outweigh the right of the public and the right of the defendant to a speedy trial, pursuant to 18 U.S.C. § 3161, *et seq.*

SO ORDERED this 12th day of September, 2023.

A handwritten signature in blue ink, appearing to read "MLB", with a long horizontal stroke extending to the right.

MICHAEL L. BROWN
UNITED STATES DISTRICT JUDGE