

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS**

UNITED STATES OF AMERICA,)
)
 Plaintiff,)
)
 v.)
)
 BRADLEY A. PISTOTNIK,)
)
 Defendant.)
 _____)

Case No.: 18-cr-10099-EFM

MEMORANDUM & ORDER ON MOTION TO QUASH SUBPOENAS

Now before the Court is the Motion to Quash Subpoenas filed by non-parties Xcentric Ventures, LL and Chandler Automated Systems (collectively “the movants”). (Doc. 47.) Having reviewed the submissions of the parties, the motion is **GRANTED in part** and **DENIED in part** for the reasons set forth below.

FACTUAL BACKGROUND

In the present action, Defendant Bradley Pistotnik has been indicted on 10 counts relating to his alleged threats to cause damage to the computer systems of Xcentric Ventures, LLC. Xcentric owns and operates a website know as www.ripoffreport.com (hereinafter “the website”), which it contends is “dedicated to consumer protection.” (Doc. 47, at 1.) Xcentric contends the website is “devoted to exposing fraudulent and improper conduct by businesses” and allows its readers to “read and post messages about businesses that purportedly have

‘ripped off’ consumers in some manner.” (*Id.*, at 1-2.) “These reports are authored and published by third-party readers and users of the Ripoff Report website, not by people employed by Xcentric Ventures.” (*Id.*, at 2.) Xcentric states that the “declare[d] ... mantra” of the website is that it “protects consumers’ first amendment right to free speech.” (*Id.*, at 1.) As such, Xcentric states that it

does not release identity information about the anonymous authors of Ripoff Reports, because Xcentric protects the free speech rights of anonymous authors, and because revealing author information without due process would chill free speech on the Ripoff Report forum and in general, due to concerns about retaliation from the subject of the Ripoff Reports.

(Doc. 47, at 2.) Xcentric also states that “[a]s part of its business practices, [it] also does not usually remove reports, but does allow for disputes about false statements of fact to be handled through a mediation program” (*Id.*, at 3.)

Chandler Automated Systems (hereinafter “Chandler”) “is a vendor of Xcentric who provides services to Xcentric in the areas of cyber security and information technology.” (*Id.*) One of Chandler’s services is to protect Xcentric from computer hackers, to which Xcentric contends it is “especially prone” as a result of “the nature of their business.” (*Id.*, at 3-4.) Chandler indicates it is a federal contractor, which requires system security plans they are involved with “to remain confidential and can only be provided to the federal government for audit purposes.” (*Id.*, at 3.) The movants contend that “[t]his confidential information

includes the internal environment of Xcentric and Chandler . . . , and release of that information would present a risk to both companies should it be obtained by hackers.” (*Id.*, at 4.)

Movants contend that an anonymous user posted a report about Defendant Pistotnik in 2014.¹ (*Id.*, at 4.) Movants continue that “[a]s alleged in the indictment, Defendant Pistotnik [sic] and Defendant David Dorsett conspired to hack and interrupt the business of Xcentric, along with its associates including its law firm of Jaburg Wilk and its customers and vendors by sending thousands of threatening messages to the servers of these businesses.” (*Id.*) Xcentric contends that the post was removed in September 2014 “to try to stop the attack,” which apparently was successful. (*Id.*) A few months later, the posting was reposted on the website, allegedly resulting in a second cyberattack. (*Id.*) Xcentric reported both sets of attacks to the FBI. (*Id.*) Movants presume that “all of the information provided to the FBI about the attacks has been provided to Defendants in discovery” following their July 2018 indictments. (*Id.*, at 5.)

The subpoenas at issue were served on the movants in September 2018 and requested a 14-day response deadline for information. The subpoena to Xcentric sought

¹ That report is referred to as “Report 1177867” in the subpoena to Xcentric and hereinafter will be referred to as “the Report.” (Doc. 47-1, at 4.)

the identity and other private information about the anonymous author of the Ripoff Report about Pistotnik; all documents that “refer to” the cyberattacks, including the details about what Xcentric did to protect itself from the attack; the identity and financial records related to the vendors Xcentric used to prevent cyberattacks; all of the information regarding the types of countermeasures used by Xcentric to prevent cyberattacks, including “the name and version number” of Xcentric’s countermeasures; documents regarding Xcentric’s web providers and hosting environment and the configuration of those systems; details about the mail servers used by Xcentric; and all data received by ripoffreport.com during the attacks.

(*Id.*, at 5; *see also* Doc. 47-1.) Movants allege that this subpoena sought “everything needed by a hacker to successfully breach all of Xcentric’s cyber security.” (*Id.*) The subpoena to Chandler requested

all mitigation, troubleshooting, investigatory or remedial steps taken by Chandler Automated Systems to help stop and mitigate the attacks on Xcentric; all information about cyberattack countermeasures available to Xcentric or its owner, Ed Magedson; the web presence provider and hosting environment information for Xcentric and its owner; all logs and data regarding email and web traffic for Xcentric, Ed Magedson or the ripoffreport.com (not limited in time or by sender); and private financial records.

(*Id.*, at 6; *see also* Doc. 47-2.) Movants contend this information, if produced, “would be sufficient to mount another attack on these entities.” (*Id.*)

ANALYSIS

I. Timeliness.

As an initial matter, Defendant argues that movants' motion is untimely because the subpoenas "provided fourteen days to respond" and neither "party asked for more time, or for clarification regarding the scope of the subpoenas" (Doc. 54, at 1.) Defendant contends that neither of the movants "took any action whatsoever, until four days after the deadline for production had passed, and then only after the undersigned filed a motion asking for a finding of contempt." (*Id.*, at 1-2.) Defendant argues that the time for movants to file a motion to quash was "*before* the due date for a response to the subpoena that is the subject of the motion." (*Id.*, at 2.) In support of this position, Defendant cites Fed.R.Crim.P. 17(c)(2), which states, "[o]n motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive."

Movants are correct that Rule 17 does not define what constitutes a "promptly" made motion. (Doc. 56, at 3.) The fourteen days was merely an arbitrary deadline Defendant imposed on complying with the third-party subpoenas. Movants indicate that they "are both out-of-state entities who were required, in order to challenge the subpoenas, to locate and retain outside counsel in Kansas." (*Id.*) The Court agrees with movants' assertion that they "filed a detailed motion to quash as fast as is reasonable under these circumstances." (*Id.*, at 4.) Further, the Court notes the irony in Defendant relying on this language from Rule 17 when Defendant blatantly failed to comply with the Rule's requirement of requesting the Court's permission before serving the third-party subpoenas. *See* Fed.R.Crim.P. 17(c)(3); *see also* n.3, *infra*. As such, the Court **OVERRULES** Defendant's timeliness argument.

II. Legal Standard on Subpoenas in Federal Criminal Cases.

Subpoenas in federal criminal matters are governed by Fed.R.Crim.P. 17.

Subsection (c) of that Rule 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. When the items arrive, the court may permit the parties and their attorneys to inspect all or part of them.

Fed.R.Crim.P. 17(c)(1).

A Rule 17(c) subpoena, however, is not “intended to provide a means of discovery for criminal cases,” but rather is intended “to expedite the trial by providing a time and place before trial for the inspection of the subpoenaed materials.” *United States v. Nixon*, 418 U.S. 683, 698-99 (1974). “In other words, Rule 17(c) is not a discovery tool but offers compulsory process for securing specific, identifiable evidence for trial.” *United States v. Jackson*, 155 F.R.D. 664, 667 (D. Kan. 1994); *see also United States v. King*, 164 F.R.D. 542, 546 (D. Kan. 1996) (holding that “Rule 17 was not intended to provide the defendant a mechanism by which to troll the waters of the seas otherwise undiscoverable material in the small hope that something beneficial might rise to the surface.”).

A subpoena for documents may be quashed if their production would be unreasonable or oppressive. Fed.R.Crim.P. 17(c)(2). *See also Nixon*, 418 U.S. at

698 (holding that “[a] subpoena for documents may be quashed if their production would be ‘unreasonable or oppressive,’ but not otherwise.”); *United States v.*

Reed, No. 06-20068-01-CM, 2008 WL 4724437, at *1 (D. Kan. Oct. 24, 2008).

To determine if the burden of compliance rises to the level of being unreasonable or oppressive, courts examine whether the party seeking for the subpoena has shown:

(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.’

Nixon, 418 U.S. at 699-700; *see also Reed*, 2008 WL 4724437, at *1. This burden on the party seeking the subpoena has been summarized as clearing the three hurdles of relevancy, admissibility, and specificity.² *Nixon*, 418 U.S. at 700. A determination of whether these hurdles have been cleared is left to the discretion of

² The Court notes that the language of the cited cases often refers to these burdens being on the “moving” party. *See e.g. Reed*, 2008 WL 4724437, at *1. That is because the party subpoenaing materials is, pursuant to Fed.R.Crim.P. 17, required to move for the Court’s permission to issue the subpoena. *Id.* In the matter before the Court, Defendant failed to do this (as discussed *supra*). As such, the Court in the present matter will discuss these burdens as they relate to the party seeking the subpoena. Simply stated, the “moving party” in the present case is not the party seeking the subpoena because of Defendant’s failure to comply with Fed.R.Crim.P. 17.

the trial court. *Jackson*, 155 F.R.D. at 667 (citing *United States v. Eden*, 659 F.2d 1376, 1381 (9th Cir. 1981)).

In determining whether the relevancy and admissibility prongs have been satisfied, courts state the requested material cannot be “potentially” relevant or admissible. *United States v. Ary*, No. 05-10053-01-JTM, 2005 WL 2372743, at *3 (D. Kan. Sept. 27, 2005) (citing *United States v. Anderson*, 31 F. Supp. 2d 933, 944 (D. Kan. 1998)). Rather, the requested material must meet the tests of relevancy and admissibility at the time they are sought. *Id.* “There must be a ‘sufficient likelihood’ that the requested material is ‘relevant to the offenses charged in the indictment,’ and a ‘sufficient preliminary showing that . . . [the requested material] contains evidence admissible with respect to the offenses charged.’” *King*, 164 F.R.D. at 545 (quoting *Nixon*, 418 U.S. at 700). Conclusory allegations of relevance and admissibility are insufficient. *Id.*, at 545.

Regarding specificity, courts note it is the most difficult hurdle to overcome. *United States v. Wittig*, 250 F.R.D. 548, 552 (D. Kan. 2008) (citing *United States v. Anderson*, 31 F.Supp.2d 933, 944 (D. Kan. 1998)). “This requirement ensures that Rule 17(c) subpoenas are used only to secure specific documents or sharply defined groups of documents for the trial.” *Ary*, 2005 WL 2372743, at *3 (citing *Anderson*, 31 F. Supp. 2d at 945). “This requirement prevents the defendant from using the subpoena as a ‘fishing expedition to see what may turn up.’” *Id.* “After

all, if the defendant cannot reasonably describe the information contained in the requested materials, but merely hopes that something beneficial will turn up, this is a sign that the Rule 17(c) subpoena is being misused.” *Id.* (citing *United States v. Jackson*, 155 F.R.D. 664, 667 (D. Kan. 1994)).

Thus, in describing the documents, the subpoena must refer to specific documents or, at least, to specific kinds of documents. *King*, 164 F.R.D. at 546. The specificity hurdle “cannot be cleared by simply naming the title of the document.” *Id.* (citing *United States v. Arditti*, 955 F.2d 331, 345–46 (5th Cir.), *cert. denied*, 506 U.S. 998, 113 S.Ct. 597, 121 L.Ed.2d 534 (1992)). Requesting entire files instead of specific documents indicates a fishing expedition. *Id.* The party seeking the documents must additionally specify why the materials are wanted, what information is contained in the documents, and why those documents would be relevant and admissible at trial. *Id.* “Conjecture and speculation will not provide the lift to carry a movant over the three hurdles.” *Jackson*, 155 F.R.D. at 668.

Movants request that the subpoenas at issue be quashed

as being unreasonable and oppressive, for seeking irrelevant and privileged matter, for requesting information that is confidential, for requesting information that is available through discovery with the United States Attorney’s office, for being used as a discovery device, and for requesting information that, if released, could expose Xcentric to another cyberattack.

(Doc. 47, at 12.) Within this context, the Court will address the various categories of information sought in the subpoenas.

III. Categories of Information Sought by Subpoenas at Issue.³

A. Subpoena to Xcentric (Doc. 47-1).

1. Information Regarding the Report (Categories 1, 2, and 3).

Categories 1, 2, and 3 of the subpoena to Xcentric seek various information about the Report against Defendant on the website. (Doc. 47-1, at 4-5.) The categories seek the author information, documents containing data collected in connection with creation of the Report (such as server logs, analytics, counters, etc.), and documents referring to the Report (including correspondence, server, logs, analytics, counters, etc.). (*Id.*) Movants argue that information regarding this Report or the anonymous poster should be quashed as irrelevant, unreasonably

³ The Court notes that Categories 9, 11, and 15 of Defendant's subpoena *duces tecum* to Xcentric (Doc. 47-1) are not discussed in the motion to quash filed by movants, nor are Categories 1-4 and 6 of Defendant's subpoena to Chandler (*see generally* Doc. 47). Typically, the Court would find that a movant waived its objections to categories of requested documents not discussed in a motion to quash a subpoena. The procedure for a subpoena in a criminal proceeding, however, requires that a subpoena may be served on a third party "only by court order." Fed.R.Crim.P. 17(c)(3). As such, Defendant was to have sought the Court's permission to serve the subpoena before doing so, which would have necessitated Defendant establish he was entitled to the information. Defendant in this instance did not seek the Court's permission pursuant to Rule 17. Further, movants' motion indicates they are moving to quash the subpoenas in their entirety. As such, the Court finds that the duty to establish whether the information should be produced is on Defendant, not the third-parties moving to quash the subpoena. *See United States v. Reed*, 2008 WL 4724437, at * 1 (citing *Nixon*, 418 U.S. at 699-700) (holding that the burden belongs to "the party moving for the subpoena").

burdensome for Xcentric to obtain the information, and “for being a thinly veiled attempt at circumventing applicable Arizona law and Xcentric’s policies.” (Doc. 47, at 7.)

Movants continue that Defendant has not given notice to the anonymous author of the report, Defendant “has not requested to give notice on the webpage,” and has not established standing to seek the author’s identity. (*Id.*, at 8.) Further, movants argue that this information is “not relevant whatsoever to the instant criminal case,” as Defendant’s “legal defense could not depend in any way on the author’s identity.” (*Id.*) Instead, movants contend that Defendant wants this information “to chill the author’s, and others’[,] free speech, and that perhaps he intends to retaliate against the author in some way.” (*Id.*, at 9.)

Defendant responds that the documents are relevant to his defense of the criminal charges he is facing. Defendant contends that he was contacted by Defendant Dorsett (hereinafter “Dorsett”) on September 12, 2014, when Dorsett solicited Defendant’s business and offered computer knowledge and skills. (Doc. 54, at 9.) During this time, Defendant was in litigation with his brother and former law partner, Brian Pistotnik. Defendant continues explaining that

as a result of the litigation and split between the two attorney brothers, the trial court ordered that a landing page be placed at ‘pistotniklaw.com,’ and that page would feature links to separate web sites for Brad Pistotnik and Brian Pistotnik, to allow equal access for

visitors to the site to select which of the Pistotnik brothers they would like to be their lawyer.

On September 14, 2014 at 3:42 p.m., Dorsett emailed Mr. Pistotnik and informed him of a ‘problem’ with the website the trial court had ordered. [Doc. 54-4.] According to Dorsett, the court-ordered website was altered in a way that would reflect that all of the website traffic was being credited to Brian Pistotnik’s web site, even when people clicked on [Defendant’s] side of the page, unfairly affecting search engine rankings in Brian Pistotnik's favor. *Id.* Dorsett told [Defendant] that he could fix this ‘problem.’ On September 14, 2014, at 3:59 PM, Dorsett emailed [Defendant] that he had never seen someone get so deliberately sabotaged, and offered to ‘fix it.’ *Id.*

Five days later, on September 19, 2014, (at approximately 10:45 a.m. CST) an anonymous negative posting regarding [Defendant] appeared on ripoffreport.com. Dorsett met with [Defendant] on September 19, 2014, approximately 15 minutes after the negative posting, to discuss an expert report that Dorsett was going to write for use in the lawsuit between [Defendant] and his brother. Dorsett also emailed [Defendant] and advised him not ‘to worry about that one [ripoffreport.com post], I have experience dealing with that site. I’ll add it to the list.’ [Doc. 54-5.] Mr. Dorsett communicated with [Defendant] stating that he had a business partner – Logan Chierotti – owned an internet reputation management company that would address the report and any others that were of concern.

(Doc. 54, at 9-10.) On September 19, 2014, Dorsett confirmed that he spoke with Chierotti, who indicated he would “remove” or “de-index” any negative reviews.

(*Id.*, at 11 (citing Docs. 54-6, 54-7).)

Defendant contends that Dorsett “had a history of seeking out people who appear to have money and sending them a message offering a way to get a page

removed for fees.” (Doc. 54, at 11.) Defendant presents evidence of this practice.

(See Docs. 54-8, 54-9.) Defendant continues that

Dorsett’s historical modus operandi of creating/seeking a ‘problem’ and then offering his services to ‘fix it’ was repeated with [Defendant] as another target. As the Government’s evidence has revealed, the ‘email bomb’ software that was used in this case was found only on Dorsett’s computer. Additionally, unbeknownst to Bradley Pistotnik, Dorsett bragged to an acquaintance to ‘extorting removals from ripoffreport.com’ via a ‘message bomb.’

(Doc. 54-10 (“I’m currently extorting removals from ripoffreport.com with it [identified as Dorsett’s ‘message bombing capabilities’] and they’re definitely looking to tie it to me”)). According to Defendant, “The solicitation of [him] by Dorsett, and Dorsett’s response to ‘not worry about it’ along with his admission of extorting ripoffreport.com tends to disprove any conspiracy.” (Doc. 54, at 12.)

The Court finds that Defendant has failed to clear the hurdles of relevancy as to the information requested regarding the anonymous Report on the website contained in Categories 1, 2, and 3 of the subpoena to Xcentric. *Nixon*, 418 U.S. at 700. Whether the posting was made by co-Defendant Dorsett or someone else is not relevant to a defense to conspiracy. Proof that Dorsett “baited” Defendant by posting the item would not legally excuse participation in the alleged conspiracy. Further, Defendant’s claim that co-Defendant Dorsett solicited his business is also

irrelevant to whether or not they committed a conspiracy. The third-party motion to quash is, therefore, **GRANTED** as to Categories Nos. 1, 2, and 3.

Further, the Court finds that the wording of Category No. 3 fails to clear the specificity hurdle, which, as discussed *supra*, is the most difficult hurdle to overcome. *Wittig*, 250 F.R.D. at 552 (citation omitted). The Category, as written, seeks “[a]ll Documents, that Refer To Report 1 17867, including any and all correspondence as well as any and all server logs, application logs, reports, analytics [sic], counters, or other Documents reflecting access to Report 1177897 by visitors to rioffreport.com.” (Doc. 47-1, at 5.) The Court finds that this category is facially overbroad as it seeks all documents that in any way “refer” to the Report at issue. This category is not “sharply defined.” *Ary*, 2005 WL 2372743, at *3 (citation omitted). Rather, the category is a more akin to a general ‘fishing expedition’ and thus prohibited under the *Nixon* specificity standard. 418 U.S. at 699-700; *see also Reed*, 2008 WL 4724437, at *1. The third-parties’ motion is **GRANTED** as to Category No. 3 on this basis as well.

2. Documents relating to Cyberattacks (Categories 4 and 5).

Category No. 4 seeks “[a]ll documents that Refer To your response to the First Attack or Second Attack.” (Doc. 47-1, at 5.) Category No. 5 asks for “[a]ll documents that Refer To the effects of the First Attack or Second Attack, including all mitigation, troubleshooting, investigatory, or remedial steps.” (*Id.*) Movants

contend that the documents requested “are privileged, or would otherwise disclose defensive architecture that needs to remain private.” (Doc. 47, at 9.) They continue that any other responsive information “was already provided to the F.B.I. and is available to Defendant in discovery.” (*Id.*) Finally, movants argue that “[c]ollecting this information would also be burdensome, including the need for a privilege review, and logging, and heavy redacting.” (*Id.*)

Defendant responds that the documents sought are “known to exist” because Xcentric provided a “portion of the server logs” to the United States. (Doc. 54, at 13.) As such, Defendant contends that he is merely “asking for the rest” of a document that has been partially provided. (*Id.*)

Defendant contends that the information is relevant because

[u]nder 18 U.S.C. 1030(a)(5)(A), which forms the basis of count five of the indictment, an element of the offense is ‘damage’ to a ‘protected computer,’ both terms of art that are defined in 18 U.S.C. 1030. ‘Damage’ is defined as ‘any impairment to the integrity or availability of data, a program, a system, or information.’ 18 USC 1030(e)(8). It is measured in dollars; the greater the amount of damage, the higher the penalty level; if the damage is not sufficient, no crime at all occurred. *See* 18 U.S.C. 1030(c)(4). The documents sought ... seek exactly the sorts of documents that explain the ‘damage’ that Xcentric supposedly suffered, as those documents will illuminate what Xcentric had to do to [sic] fix the damage. The \$72,000.00 of damage Xcentric claims it suffered is a big number that has big consequences under the Computer Fraud and Abuse Act. The relevance of the documents illuminating what ‘damage’ that

\$72,000.00 was incurred to fix and whether it was actually paid is both obvious and critical.

(*Id.*, at 14.) Defendant argues that because the documents are relevant, Xcentric’s burdensome objection “is reduced to nothing more than a complaint that responding to a subpoena takes effort that Xcentric wouldn’t otherwise be required to expend.” (*Id.*, at 15.)

The Court reads Categories 4 and 5 as seeking documentation underlying Xcentric’s claimed damages. To this end, Defendant has included a copy of Xcentric’s invoice for \$72,261.50 in its responsive brief. (*Id.* 54, at 13.) Defendant is now merely requesting backup on information on this particular invoice. The underlying documentation of the victim’s damages is relevant – and to the extent Categories 4 and 5 intend to seek such documents, the requests are relevant. The Court also finds that Categories 4 and 5 clear the hurdles of admissibility and specificity. As such, the Court **OVERRULES** Xcentric’s overly burdensome objection and **DENIES** the motion to quash as to Categories 4 and 5.

3. Categories 6, 7, and 8.

Category No. 6 asks for all documents referring to the removal of the Report from the website in September 2014, “including the reasons for the removal and the date and time of the removal.” (Doc. 47-1, at 5.) Category No. 7 seeks all documents referring to “the re-posting” of the Report on the website in June 2015, “including the reason for the re-posting and the date and time of the re-posting.”

(*Id.*) Category No. 8 asks for all documents referring to Defendant, “including all correspondence between You and any other Person.” (*Id.*)

Movants argue that the categories “request privileged information, are irrelevant to the criminal case, and collection of the information would be burdensome, including the need for privilege review and logging, as well as redaction of confidential and technical information.” (*Id.*) Defendant’s response brief does not address these categories. As such, Defendant has failed to clear the hurdles of relevance, admissibility, and specificity regarding this information. Movants’ motion is **GRANTED** as to Categories 6, 7, and 8.

4. Cyberdefenses (Categories 10, 12, 13, and 14).

These categories ask Xcentric to provide information regarding the architecture of its cyberdefenses. Movants argue that “[i]t is not safe for Xcentric to publicly disclose all of the technical information about its technical defenses to cyberattack” because this would “allow evildoers to analyze them, and more efficiently defeat them.” (Doc. 47, at 10.) Movants continue

Information about the configuration of Xcentric’s cyber defenses make no difference at all to the facts at issue in the instant case. Defendant attacked Xcentric and overwhelmed key email inboxes and demanded that Xcentric take down user generated content from RipoffReport.com. To stop the attack, Xcentric removed user generated content. Nothing about Xcentric’s cyber defenses would be at issue in this case.

(*Id.*)

Defendant responds that the requested information is “eminently relevant” given the “outlandishly high” amount of movants’ claimed damages.

Every web host has the systems that are referred to in these portions of the subpoenas, and all of the documents sought by the requests Xcentric cites are relevant to the question of damages. Damage, recall, is defined as actual impairment to the integrity or availability of a protected computer. 18 U.S.C. 1030(e)(8). This request seeks shed light on the characteristics of the ‘protected computer(s)’ affected by the attack, as well as how they were affected by the attack. It has been claimed, variously, that the attacks consisted of ‘dozens,’ ‘hundreds,’ or as many as 14,000 emails. The mail server logs will clarify that number. And the documents regarding spam and DDoS countermeasures will clarify how, exactly, those emails – be they dozens, hundreds, and thousands – somehow managed to cause 72,000.00 in damage.

(Doc. 54, at 16.)

The Court finds that information relating to cyberdefenses is irrelevant. The information is simply not necessary, or related, to providing or disproving movants’ alleged damages. Comparative fault is not a defense. Further, Defendant has not addressed the admissibility of the requested information. Even assuming the information is admissible, the Court finds that Categories 10, 12, 13, and 14, as worded, fail to meet the specificity requirement.

As stated above, the specificity hurdle ensures that Rule 17(c) subpoenas are used only “to secure specific documents or sharply defined groups of documents for the trial.” *Ary*, 2005 WL 2372743, at *3 (citing *Anderson*, 31 F. Supp. 2d at

945). “This requirement prevents the defendant from using the subpoena as a ‘fishing expedition to see what may turn up.’” *Id.* Categories 10, 12, 13, and 14, as worded, read like standard document requests sent in civil discovery or language included in a subpoena *duces tecum* for a discovery deposition in a civil case. In that context, the categories would, most likely, not be objectionable. As stated above, however, a Rule 17(c) subpoena, however, is not “intended to provide a means of discovery for criminal cases,” but rather is intended “to expedite the trial by providing a time and place before trial for the inspection of the subpoenaed materials.” *United States v. Nixon*, 418 U.S. at 698-99.

It is well-established that Rule 17(c) “is not a discovery tool but offers compulsory process for securing specific, identifiable evidence for trial.” *United States v. Jackson*, 155 F.R.D. 664, 667 (D. Kan. 1994). Language such as “all documents” that “refer” to a particular topic or “include,” but are not limited to, certain types of documents, as used in these categories, clearly reads like discovery requests and does not identify “specific documents or sharply defined groups of documents for the trial.” *Ary*, 2005 WL 2372743, at *3. As such, these categories are improper and the Court **GRANTS** movants’ motion as to Categories 10, 12, 13, and 14.

B. Subpoena to Chandler (Doc. 47-2).

Movants argue that “the subpoena to Chandler Automated Systems carry

with them the same dangers, as well as similar unnecessary and unfair burdens, as the requests to Xcentric.” (Doc. 47, at 10.) While movants are seeking to have the Chandler subpoena quashed in its entirety, they specifically discuss three of the eight categories of information requested.

Category No. 5 seeks all documents referring to “either the web presence provider, the hosting environment ..., or any third-party DNS service ... used by Xcentric ..., and the configuration of the same at the time of the First Attack or Second Attack.” (Doc. 47-2, at 5.) Movants argue that

[p]ublishing this information would present a great risk to the security of the existing systems, and require Chandler to replace or change all of those system to protect Xcentric and other clients. Because Chandler Automated Systems is a federal contractor, the system security plans is required to be confidential/classified and can only be provided to the Federal Government for audit purposes under FedRAMP/FISMA guidelines.

(Doc. 47, at 11.)

Category No. 7 asks for “[a]ll mail server or e-mail-related logs, reports, data, or analytics that Refer To email or web traffic received by Xcentric ... in September of 2014 or July of 2015.” (Doc. 47-2, at 5.) Movants argue that “the logs contain classified information about the internal environment of Chandler Automated Systems and Xcentric Ventures that would present a risk if provided to potential attackers, especially if the attackers have previously attacked the system.”

(Doc. 47, at 11.)

Finally, to Category No. 8 requests “[c]heck stubs, transaction records, and other backup for any payments you received from Xcentric ... related to either the First Attack or the Second Attack.” (Doc. 47-2, at 5.) Movants contend that “portions of the invoices submitted to Xcentric Ventures provide information about systems put in place to protect Xcentric and provides information that an attacker can use to develop explicit attack vectors to Chandler Automated Systems.” (Doc. 47, at 11.) They argue that “[t]his information is also part of the Federally Protected/ Classified System Security plan.” (*Id.*)

Defendant’s response in opposition to the motion to quash contains no substantive discussion of the categories of information sought in the Chandler subpoena. (*See generally* Doc. 54.) Instead, Defendant merely argues that “as to Chandler, the motion is not even properly before the Court.” (Doc. 54, at 17.) Defendant argues that “no request for relief is properly before the Court, as Chandler’s attitude toward the subpoena is so dismissive it hasn’t even deigned to enter an appearance.” (*Id.*, at 2.)

Defendant’s argument that the motion is not properly before the Court as to the Chandler subpoena is misplaced. The Court is more concerned with Defendant’s dismissive attitude towards Fed.R.Crim.P. 17, as Defendant failed to seek the Court’s permission before serving the third-party subpoena on Chandler. Further, Xcentric has standing to challenge the subpoena to Chandler because it

has a personal right or privilege with respect to the subject matter of the information requested in the subpoena. *See, e.g., Holick v. Burkhardt*, No. 16-1188-JTM-KGG, 2017 WL 3723277, at *5 (D. Kan. Aug. 28, 2017) (quoting *Smith v. Midland Brake, Inc.*, 162 F.R.D. 683, 685 (D. Kan. 1995)).

Because Defendant's responsive brief makes no substantive discussion of the categories of documents sought by the Chandler subpoena, Defendant has thoroughly failed to address the three hurdles of relevancy, admissibility, and specificity in regard to the Chandler subpoena. *Nixon*, 418 U.S. at 700; *see also Reed*, 2008 WL 4724437, at *1. As such, Defendant cannot meet his burden and the Motion to Quash (Doc. 47) is **GRANTED** as to the Chandler subpoena.

IT IS THEREFORE ORDERED that the non-parties' Motion to Quash Subpoenas (Doc. 47) is **GRANTED in part** and **DENIED in part** as more fully set forth above.

IT IS FURTHER ORDERED that the documents to be produced in accordance with this Order shall be submitted to the chambers of the undersigned Magistrate Judge at the United States District Courthouse for the District of Kansas, Wichita Division, 401 N. Market, Suite 401, Wichita, Kansas, 67202 on or before 10:00 a.m. on March 13, 2019. Chambers will then arrange for defense counsel to inspect the documents.

IT IS SO ORDERED.

Dated this 12th day of February, 2019, at Wichita, Kansas.

S/ KENNETH G. GALE
HON. KENNETH G. GALE
U.S. MAGISTRATE JUDGE