IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

QUETEL CORPORATION,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Civil Action No. 1:17cv0471 (AJT/JFA)
	)	
HISHAM ABBAS, *et al.*,	)	
	)	
Defendants.	)	
	)	

PROPOSED FINDINGS OF FACT AND RECOMMENDATIONS

This matter is before the court on plaintiff QueTel Corporation's ("plaintiff" or "QueTel") motion for sanctions for destruction or suppression of discoverable materials and for failure to comply with a court order. (Docket no. 35). Since a portion of plaintiff's motion seeks relief that would be dispositive of one or more claims in the complaint, it is being considered in accordance with 28 U.S.C. § 636(b)(1)(B). Pursuant to 28 U.S.C. § 636(b)(1)(C), the undersigned magistrate judge is filing with the court his proposed findings of fact and recommendations, a copy of which will be provided to all interested parties.

Factual Background

As alleged in its complaint (Docket no. 1) ("Compl."), plaintiff has spent several years developing a portfolio of evidence management and asset tracking software solutions for law enforcement agencies. (Compl. ¶¶ 18–20). This portfolio includes several "modules" which allow for a wide range of evidence management and asset tracking, including physical evidence management, laboratory management, digitized paper records, inventory management, and a mobile application which allows for the uploading of live evidence. (Compl. ¶ 20). Each module is connected to one core source code (the "Core Engine") that coordinates the software's

overall functionality by harmonizing the working of the modules to promote a seamless user experience. (Compl. ¶ 22). A user interacts with the modules rather than the Core Engine itself, which can be accessed on a web-browser using a graphic user interface through a computer or smart device. (*Id.*). The Core Engine allows QueTel to add new modules to its customers' systems quickly because each module relies on the same Core Engine to control user permissions, data entry, data access, and other features needed for the modules to function. (Compl. ¶ 26). The portfolio of modules, the Core Engine, and the associated graphic user interface are referred to as the TraQ Suite. (Compl. ¶ 22).

In late 2010, following a year of development, QueTel deployed the Core Engine and its components for use by a customer for the first time. (Compl. ¶ 29). Between 2010 and April 2016, QueTel added approximately thirty add-on features and made over 100 changes to the source code. (Compl. ¶ 30). The current TraQ Suite version at issue in this litigation is called "TraQ Suite 6." (Compl. ¶ 31). There are over 2,200 files of computer source code comprising TraQ Suite 6. (Compl. ¶ 32). QueTel obtained a copyright registration for the TraQ Suite 6 code on or about March 21, 2016 with the United States Copyright Office. (Compl. ¶ 37).

QueTel's customers do not have access to the TraQ Suite 6 source code, but instead they interact with TraQ Suite 6's modules through web-browsers using an executable program. (Compl. ¶ 38). The executable program used by the customer cannot reveal the source code for TraQ Suite 6 and the customer has no means of accessing the code for TraQ Suite 6 and cannot copy, reverse engineer, decompile, or disassemble the TraQ Suite 6 code. (*Id.*). The TraQ Suite 6 code resides at all times with QueTel, and cannot be obtained by the public or QueTel's competitors through lawful means. (*Id.*).

In June 2007, plaintiff hired defendant Hisham Abbas to help develop QueTel's first generation browser application for evidence tracking and inventory management. (Compl. ¶¶ 12, 28). Abbas became the lead software developer at QueTel in June 2013. (Compl. ¶ 3). During the period in which Abbas served as QueTel's lead software developer, he maintained a complete copy of the TraQ Suite 6 source code on his work issued laptop computer. (Compl. ¶ 55). In April 2014, Abbas resigned from QueTel. (Compl. ¶ 56).

In January 2014, prior to his resignation from QueTel, Abbas co-founded defendant finalcover, LLC with his wife, defendant Shorouk Mansour (collectively "defendants"). (Docket no. 36 at 4, Exhibit B). Abbas publicly identifies himself as the CEO and co-founder of CaseGuard | finalcover as of January 1, 2014. (Docket no. 36 at 4, Exhibit A). Defendants registered the <CaseGuard.com> domain name on or about May 28, 2014. (Docket no. 9 at 17). Defendants state that in May 2014, Abbas began to develop CaseGuard, a web-based evidence management software program. (Docket no. 42 at 8). Like TraQ Suite 6, CaseGuard's code resides with finalcover while customers access modules through a web-browser. (Docket no. 42 at 8–10). In January 2015, defendants launched a website at www.CaseGuard.com advertising three modules. (*Id.* at 10). Defendants maintain that at the time the website was launched, it was merely a shell and the modules were not fully functional. (*Id.*).

Plaintiff alleges that defendants misappropriated its TraQ Suite 6 source code and used it to create CaseGuard. (Compl. ¶ 63). Plaintiff sent defendants a cease and desist letter on May 16, 2016. (Compl. ¶ 81; Docket no. 42-10). In that letter, plaintiff demanded that defendants: (1) cease infringing on plaintiff's intellectual property including the computer software source code underlying the TraQ Suite 6 software, (2) cease all advertising, promotion, and sale of the CaseGuard software, (3) provide an accounting of all sales of the CaseGuard software made to

date; and (4) allow plaintiff to copy and inspect a complete copy of all versions of the CaseGuard source code as well as any computers that Abbas used during the period from January 1, 2014 to present. (Docket no. 42-10). Plaintiff's cease and desist letter also included the following lengthy paragraph setting forth a request that information be preserved:

> Beyond the above-referenced obligations, **please be aware that you must preserve all potentially relevant evidence relating to the matters addressed in this letter.** This duty to preserve potentially relevant evidence extends to all such evidence, regardless of the format in which it may exist. It specifically includes, but is not limited to, any e-mails (whether in a personal or business e-mail account), any documents stored on any personal or business computers, servers, electronic storage devices, external hard-drives, or other similar devices, and/or cloud storage accounts concerning the subject matter of this letter, CaseGuard and/or TraQ Suite 6. Failure to preserve such evidence may result in sanctions. The possible sanctions include an inference in judicial proceedings that the failure to preserve such evidence indicates knowledge of wrongdoing and liability, and that any destroyed evidence would have helped establish the Company's claims, as well as monetary and other judicially imposed sanctions.

(*Id.* at 4–5) (emphasis in original). Defendants' counsel responded to the plaintiff's letter on May 17, 2016, stating that QueTel's claim of infringement was without merit and that the defendants were not willing to comply with any of the plaintiff's demands. (Docket no. 42-11).

As set forth in an August 31, 2017 letter from defendants' counsel to plaintiff's counsel, Abbas purchased a new computer around September 2016 and "he disposed of his 'old computer' in late 2016." (Docket no. 36-4 at 18–21). It is also undisputed that the computer that was "disposed of" in late 2016 was the computer that Abbas used to develop CaseGuard. (Docket no. 42 at 11). Abbas states that in 2016 when he replaced the computer used to develop CaseGuard, he "transferred files from his old computer to his new computer." (*Id.* at 15).

The evidence has established, and defendants now acknowledge, that the computer Abbas used to develop CaseGuard did have Git BASH, a source code control system, installed on it

while Abbas was developing CaseGuard.[1] (Docket no. 42 at 9). Abbas has also recently admitted that not only was Git BASH installed on the computer he used to develop CaseGuard, but that he tried it for a short period of time during the development of CaseGuard but he did not like it. (*Id.*). Plaintiff argues that defendants must have used a source code control system in developing CaseGuard, while defendants claim that they did not use one. (Docket nos. 36 at 2–3, 42 at 9). A source code control system is a version control system which contains all prior versions and changes to a software's source code, thereby enabling a developer to review previous iterations of a program's code. If defendants used a source code control system to develop CaseGuard, it would contain a historical record of previous versions and changes made to the code, which could help establish whether CaseGuard was derived from TraQ Suite 6. Even if a source code control system was not used throughout the development of CaseGuard, it would provide information concerning the status of the source code development during the period of time it was in use. The parties agree that the source code control system that was installed on the computer used by Abbas to develop CaseGuard is lost and it cannot be restored or replaced through additional discovery.

Procedural Background

On April 19, 2017, plaintiff initiated this action against defendants, alleging copyright infringement (Count I), misappropriation of trade secrets (Count II), violation of the Virginia Computer Crimes Act (Count III), breach of the duty of loyalty (Count IV), breach of contract (Count V), tortious interference with contract and business expectancies (Count VI), conversion

[1] Defendants represented as late as July 13, 2017 that not only did they not use a source code control system in developing CaseGuard, they never had a source code control system. (Docket no. 36-10 at 2) ("finalcover is a small company. They do not use multiple developers. It never had a source code control system.").

(Count VII), and business conspiracy (Count VIII). (Compl. ¶¶ 88–168). On June 5, 2017, discovery opened with discovery to be completed by October 13, 2017. (Docket no. 10).

On July 14, 2017, plaintiff filed a motion to compel documents and information regarding, among other things, previous versions of defendants' source code, any source code control system used in the development of CaseGuard, and forensic images of all electronic devices used in the development of CaseGuard. (Docket nos. 19; 20 at 4, 8). On July 21, 2017, this court granted in part plaintiff's motion to compel, ordering defendants to produce the source code control system—to the extent one was used—as well as forensic images of the devices used to develop CaseGuard. (Docket nos. 29, 31 at 18:20–19:11).[2] In response to a court order, defendants produced a forensic image of a hard drive on July 28, 2017 and a forensic image of a second hard drive on August 2, 2017. (Docket no. 36 at 8). An examination of these two hard drives by plaintiff's expert revealed that they were from a device that was first used in September 2016. After this was brought to defendants' attention, they admitted that the computer used in the development of CaseGuard had been "disposed of" in late 2016. Defendants did not produce any source code control system in response to plaintiff's discovery requests and the court's order, again claiming that Abbas did not use one to develop CaseGuard. (Docket nos. 36 at 8, 42 at 14–15). Defendants have failed to address the issue that even if a source code control system was used for a short period of time, as they now admit, it would have captured a version of the source code during that part of the development phase and would be relevant to the issues involved in this litigation.

[2] At no point during the briefing or argument relating to this motion to compel did the defendants inform the plaintiff or the court that the computer used to develop CaseGuard had been "disposed of."

On September 22, 2017, plaintiff filed this motion for sanctions claiming that defendants failed to preserve not only the computer used to develop CaseGuard, but they had also deleted a source code control system and thousands of CaseGuard-related files from the new computer in July 2017, just days prior to the forensic copies of the hard drives from that computer being made and produced to the plaintiff. (Docket no. 35). Defendants filed their opposition to the motion on October 6, 2017 (Docket no. 42), and plaintiff filed a reply on October 11, 2017 (Docket no. 49). In the reply, plaintiff raised the issue that in a deposition taken on October 10, 2017, it first learned that as many as seven or eight computers were used in developing CaseGuard but the defendants produced forensic images from only one computer. (Docket no. 49 at 4). On October 13, 2017, the parties appeared before the undersigned to present argument on plaintiff's motion. (Docket no. 50).

Proposed Findings and Recommendations

Plaintiff alleges that defendants intentionally destroyed or failed to preserve material evidence and that they did not comply with this court's order on its motion to compel (Docket no. 29). As explained in more detail below, it is recommended that there be a finding that the defendants engaged in both forms of misconduct.

Failure to Preserve

Federal Rule of Civil Procedure 37(e) provides that if a party fails to take reasonable steps to preserve electronically stored information that should have been preserved in the anticipation or conduct of litigation, and that information cannot be restored or replaced through additional discovery, the court: "(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or (2) only upon finding that the party acted with the intent to deprive another party of the information's use

in the litigation may: (A) presume that the lost information was unfavorable to the party; (B) instruct the jury that it may or must presume the information was unfavorable to the party; or (C) dismiss the action or enter a default judgment." The duty to preserve evidence arises not only during litigation, but also extends to the period before litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation. *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001). District courts have broad discretion in imposing sanctions where spoliation occurs. *BMG Rights Mgmt (US) LLC v. Cox Communications, Inc.*, 199 F. Supp. 3d 958, 986 (E.D. Va. 2016) (citing *Turner v. United States*, 736 F.3d 274, 281 (4th Cir. 2013)).

As stated in the advisory committee notes, Rule 37(e) was amended in 2015 to address a circuit split regarding the different standards applied for imposing sanctions on parties who failed to preserve electronically stored information. In cases where a court does not find that a party acted with the intent to deprive the opposing party of evidence, courts should exercise restraint and only authorize sanctions that are "no greater than necessary to cure the prejudice" caused by the party's misconduct. However, on a finding that a party acted with the intent to deprive another party of the information's use in the litigation, courts are authorized to consider more severe sanctions. Even where a party acted willfully, courts should exercise restraint in imposing sanctions and the remedy should fit the wrong, and the severe measures authorized by in Rule 37(e)(2) should not be used when the information lost was relatively unimportant or lesser measures such as those specified in subdivision (e)(1) would be sufficient to redress the loss.

In addressing the issue of whether plaintiff is entitled to sanctions under Rule 37(e), the court must first determine whether the defendants had a duty to preserve the computer used to

develop CaseGuard, the source code control system that was installed on the replacement computer, and the thousands of CaseGuard-related files that were deleted from the replacement computer. There is no bright line rule regarding the duty to preserve; rather, a court must determine when a party is reasonably on notice of potential litigation. *See Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (noting that plaintiff's counsel "recognized not only that they would be suing [defendant], but also that [defendant] should be given an opportunity to inspect the vehicle").

Having reviewed the May 16, 2016 letter sent to the defendants, the pleadings filed by the parties, and having heard the arguments of counsel, it is recommended that the court find that as of May 16, 2016 the defendants were on notice of potential litigation and that they had a duty to preserve the computer used to develop CaseGuard and all information relating to the development of CaseGuard. On May 16, 2016, counsel for the plaintiff sent the defendants a cease and desist letter, which stated in part: "**please be aware that you must preserve all potentially relevant evidence relating to the matters addressed in this letter**. . . . [The duty to preserve] specifically includes, but is not limited to . . . any documents stored on any personal or business computers, servers . . . concerning the subject matter of this letter, CaseGuard and/or TraQ Suite 6." (Docket no. 42-10 at 4) (emphasis in original). The cease and desist letter was detailed, specific, and clear. It addressed the need to preserve all information concerning the development of CaseGuard and specifically referenced a request to allow plaintiff to copy and inspect "a complete copy of all versions of the CaseGuard source code as well as any computers that Abbas has used during the period from January 1, 2014 to present." (*Id.*). There can be no credible argument that the May 16, 2016 letter did not put the defendants on notice of potential litigation concerning the development of the CaseGuard source code and that the computer used

to develop CaseGuard should be preserved. *See Goodman v. Praxair Services, Inc.*, 632 F. Supp. 2d 494 (D. Md. 2009) (finding that a pre-filing letter between litigants provided constructive notice that litigation was likely).

It was neither unreasonable nor disproportionate to expect defendants to abstain from destroying a computer which could have easily been stored or otherwise preserved even if a newer one was being used in its place. The defendants' argument that the computer used to develop CaseGuard was not destroyed until several months after the cease and desist letter was received absolves them of responsibility is without merit. The cease and desist letter was received by the defendants on May 16, 2016 and they retained a lawyer to respond to that letter. Four months later they obtained a new computer and transferred "files" from the computer used to develop CaseGuard to this new computer. Thereafter the computer used to develop CaseGuard was "disposed of." The defendants' destruction of the computer used to develop CaseGuard within several months of receiving plaintiff's cease and desist letter placing them on notice of plaintiff's claims and requesting that they preserve relevant evidence was not reasonable. Therefore, it is recommended that there be a finding that the defendants had a duty to preserve the computer used by Abbas to develop CaseGuard, that they failed to take reasonable steps to preserve it, and that the information on that computer cannot be restored or replaced through additional discovery.

In addition to the destruction of the computer used to develop CaseGuard prior to the initiation of this action, plaintiff claims that in July 2017 the defendants uninstalled a source code control system that had been installed on the replacement computer in September 2016 when the files were transferred from the computer that was destroyed in late 2016. (Docket no. 36 at 16). This deletion of the source code control system occurred just days before the defendants had the

forensic image of the hard drives prepared for production to the plaintiff and was long after the issue of whether a source code control system had been used by the defendants in the development of CaseGuard had been raised during discovery. (*Id.*). The defendants were clearly on notice that any such system should be preserved but instead they removed the source code control system from the replacement computer prior to making a forensic image. Plaintiff has also provided evidence showing that thousands of CaseGuard-related files were deleted from the "backups" folder of the replacement computer a few weeks before the forensic images were prepared for production to the plaintiff and long after the defendants had been served with discovery requests concerning all CaseGuard-related files. (*Id.* at 17).

Defendants' response to the destruction of this evidence is somewhat confusing. At one point they state that they did not refuse to produce their source code control system because they no longer possess the computer used to develop CaseGuard. (Docket no. 42 at 13, 15). But later they admit that the Git source code control system had been installed on the replacement computer and they uninstalled that system on July 20, 2017 prior to the forensic images being prepared. (*Id.* at 15, 24). Defendants claim that they uninstalled the source code control system because it had not been used in the development of CaseGuard (having earlier admitted that it had been used for a short period of time) and then seem to seek solace in saying that it was uninstalled the day **before** the court entered an order requiring a forensic image be produced. (*Id.* at 15, 24).[3] As to the deletion of thousands of CaseGuard-related files on July 1, 2017, defendants claim that they may have been deleted when Abbas made a copy and re-uploaded

[3] Defendants overlook the fact that they had been served with discovery requests that would have included that information and that prior to the removal of the source code control system the defendants had agreed to withdraw their objection to document requests seeking a forensic image of each computer/server used for the production operation of the Target System. (Docket no. 36-7 at 24, Letter dated July 17, 2017, Docket no. 36-8).

CaseGuard's code to counsel's cloud drive. (Docket no. 42 at 16). Given that the deletion of the files occurred on July 1, 2017, the events described by the defendants on July 14, 2017 provide no credible explanation for the deletion of those files. Even if some or all of those files may have been duplicates, that does not justify the deletion of those files during litigation. Defendants have not given a satisfactory explanation for deleting the source code control system or the thousands of CaseGuard-related files from the replacement computer while this litigation was pending.

Second, plaintiff has been prejudiced by defendants' misconduct. Had defendants preserved the computer used to develop CaseGuard, plaintiff would know how long the source code control system was used and it could conduct a line-by-line comparison of earlier versions of the code in order to determine whether the CaseGuard code was derived from the TraQ Suite 6 code. (Docket no. 34 at 20). This would be true even if the source code control system had only been used for one or two months as testified to by Abass since it would have captured the version of the source code in existence at that time. (Docket no. 49 at 2). Instead of having this direct evidence, plaintiff is required to build a substantially circumstantial case through the use of expert testimony which cannot match the strength of a case built on a direct comparison of the code as it was being developed by the defendants.[4] Moreover, if defendants had properly preserved the computer used to develop CaseGuard it may have supported their argument that Abbas did not employ a source code control system for any significant period of time, even though it would have provided some evidence of prior versions of the source code. Furthermore,

[4] It cannot go without noting that the plaintiff does have one strong piece of direct evidence that the defendants had access to and were using the TraQ Suite 6 code in developing the CaseGuard code. In July 2014 Abbas inadvertently sent an employee of QueTel a screen shot from the computer Abbas was using to develop CaseGuard showing that a source code control system was being used and that the CaseGuard source code exhibited on the screenshot is substantially the same as the TraQ Suite 6 source code. (Compl. ¶¶ 66–77).

the defendants repeated denial of the existence or any use of a source code control system required the plaintiff to incur significant expense in litigating the very existence of the source code control system. Similarly, the source code control system that was installed on the replacement computer when the files were transferred from the computer used to develop CaseGuard would have likely contained at least some relevant information concerning the development of CaseGuard. While it is clear that thousands of CaseGuard-related files were also deleted from the replacement computer in July 2017, at this point it is unclear if those were duplicates of files that remained and were produced to the plaintiff or if they were additional files that could show the development of the CaseGuard code. In any event, there is no reason why the defendants should have deleted those files and they should bear the consequences of their actions. For these reasons it is recommended that the court find that plaintiff has been prejudiced by defendants' failure to preserve electronically stored evidence in violation of Rule 37(e)(1) and that plaintiff is entitled to sanctions.

Based on the record presented involving this motion, it is also recommended that plaintiff is entitled to sanctions pursuant to Rule 37(e)(2). Rule 37(e)(2) requires that a party act with the intent to deprive another party of the information's use in the litigation. While courts should be cautious in inferring this intent and avoid having unintentional spoliation be treated as intentional destruction of evidence, the facts in this case more than justify a showing of intentional destruction of evidence. The evidence of defendants' bad faith intent highlighted by plaintiff includes: (1) the complete destruction of the computer used to develop CaseGuard in late 2016 despite receiving the cease and desist letter only a few months prior to that destruction; (2) deleting the source code control system and thousands of CaseGuard-related files from the replacement computer in July 2017 while the parties were in the midst of serious discovery

disputes; (3) the defendants' lack of candor in disclosing the destruction of the computer used to develop CaseGuard; (4) the repeated denials of the existence of a source code control system; (5) the representations that a source code control system was not used in the development of CaseGuard when in fact it was used for at least a short period of time; and (6) the failure to disclose and provide forensic copies of all the computers used to develop CaseGuard. (Docket nos. 36 at 22–23, 49 at 4). Defendants' justifications for those instances are that: (1) Abbas kept his six-year-old computer for a few months after receiving the cease and desist letter and then decided to destroy it because he no longer anticipated litigation; (2) defendants did not use the Git source code control system throughout the development of CaseGuard, and its destruction did not prevent plaintiff from obtaining the information needed to prosecute its case; and (3) defendants did not delete thousands of files—the purported deletion was due to Abbas re-uploading CaseGuard's code to Dropbox as requested by counsel, and then deleting the original upload. (Docket no. 42 at 15–16, 32). Defendants' explanations fail to justify any of their conduct.[5]

Plaintiff points to *BMG Rights Mgmt. (US) LLC v. Cox Communications, Inc.*, Civil Action No. 1:14-cv-1611 (E.D. Va. Oct. 22, 2015) as an analogous case regarding the intent required for Rule 37(e)(2) sanctions. In *BMG Rights*, this court found that the evidence clearly revealed that the plaintiffs were preparing for and anticipating filing suit against the defendants since at least early 2013 and therefore had a duty to preserve material evidence. No. 1:14-cv-1611, slip op. at 4. Despite clearly anticipating the filing of a lawsuit by the plaintiffs which would involve the reliability of a program used by their agent, the plaintiffs' agent altered,

[5] For example, during his deposition on October 11, 2017, Abbas explained that he wiped his computer before throwing it in a commercial trashcan. (Docket no. 49 at 7). Defendants offered no justification for this action mere months after receiving a cease and desist letter from plaintiff.

deleted, and overwrote portions of a critical software program's source code without maintaining a record of those changes. *Id.* The failure to maintain a record of the changes made to the software's source code limited the defendants' ability to determine how that software program operated during the relevant time period which may have severely undermined the plaintiffs' claims. *Id.* at 3.

Defendants' conduct in this action is at least as egregious as that described in *BMG Rights*. Defendants inexplicably destroyed the computer used to develop CaseGuard in late 2016 after receiving a cease and desist letter placing them on notice of the potential litigation and requesting that information be preserved. Once litigation was instituted, the defendants failed to inform the plaintiff or the court of the destruction of that computer until plaintiff's expert raised the issue following a review of the forensic copies of the two hard drives defendants produced. During the middle of discovery in July 2017 the defendants deleted the source code control system and thousands of CaseGuard-related files that were on the replacement computer. Those actions, along with defendants' lack of candor during this litigation strongly support a finding of an intent to destroy relevant evidence in order to prevent plaintiff from obtaining it, thereby entitling plaintiff to sanctions under Rule 37(e)(2).

Failure to Comply with a Court Order

Federal Rule of Civil Procedure 37(b)(2)(A) provides that if a party fails to obey an order to provide or permit discovery:

> [T]he court where the action is pending may issue further just orders. They may include the following:
> (i) directing that the matters embraced in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims;
> (ii) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence;

> (iii) striking pleadings in whole or in part;
> (iv) staying further proceedings until the order is obeyed;
> (v) dismissing the action or proceeding in whole or in part;
> (vi) rendering a default judgment against the disobedient party; or
> (vii) treating as contempt of court the failure to obey any order except an order to submit to a physical or mental examination.

As an initial matter, defendants failed to obey an order to provide or permit discovery as required by Federal Rule of Civil Procedure 37. This court's order required defendants to produce documents and data responsive to plaintiff's Requests for Production nos. 5, 44, and 45, which sought:

- No. 5: All software (including executable, interpreted, source code, and/or otherwise) for the production operation of all versions of the Target System.
- No. 44: The complete source code control system (whether created by Subversion, Microsoft Source Safe, Git, or some other application) for the Target System.
- No. 45: A forensic image of each computer/server used for the production operation of the Target System including application, database, and any other servers. If such computers/servers contain multiple storage devices, each storage device shall be imaged. The forensic image(s) shall be produced in a format compatible with EnCase.

(Docket nos. 31 at 18:20–19:1; 36-6 at 9, 14). This court also noted that the source code control system should be produced "to the extent that there is a source code system . . . ." (Docket no. 31 at 19:5–11). Defendants ultimately provided forensic images of two hard drives from the replacement computer, but did not produce the source code control system that had been on that computer, alleging that Abbas never used one. (Docket nos. 36 at 8, 42 at 14–15). In addition, Song Song, an engineer for finalcover who worked on the development of CaseGuard, stated during his deposition on October 10, 2017 that he used a computer belonging to finalcover, and that there were as many as seven or eight computers used by finalcover's engineers to develop

CaseGuard. (Docket no. 49-4 at 7–8). Defendants never produced forensic images of those computers, despite being explicitly instructed by the court to produce forensic images of all equipment used to develop CaseGuard. (Docket no. 31 at 18:20–19:11). Therefore, it is also recommended that there be finding that the defendants violated this court's order granting in part the plaintiff's motion to compel dated July 21, 2017 (Docket no. 29), by failing to produce forensic images of all computers used in the development and operation of CaseGuard.

Sanctions

As an initial matter, the sanctions authorized by Rules 37(b)(2)(A) and 37(e) are effectively the same. Plaintiff suggests four potential remedies authorized by Rules 37(b)(2)(A) and 37(e), seeking that the court: (1) enter a finding of liability as to Counts I and II of the complaint; (2) direct that it be taken as established in this case that defendants misappropriated and copied TraQ Suite 6, and that CaseGuard and TraQ Suite 6 are substantially similar, both objectively and subjectively;[6] (3) preclude defendants from putting on any evidence that they did not copy plaintiff's source code, or misappropriate plaintiff's trade secrets; and/or (4) enter an order requiring that certain jury instructions be given at the trial in this matter. Plaintiff also seeks an award of attorney's fees, costs, and expert expenses incurred due to defendants' misconduct. (Docket no. 35 at 1–2). In its motion and at the hearing held on October 13, 2017, plaintiff stated its preference for a finding of liability as to Counts I and II of its complaint for copyright infringement and misappropriation of trade secrets.

In determining the appropriate sanction, "[t]he remedy should fit the wrong, and the severe measures authorized by [Rule 37(e)(2)] should not be used when the information lost was relatively unimportant or lesser measures such as those specified in subdivision (e)(1) would be

[6] The undersigned notes that plaintiff's second proposed remedy would in essence have the same effect as a finding of liability as to Counts I and II of plaintiff's complaint.

sufficient to redress the loss." Fed. R. Civ. P. 37(e) advisory committee's note to 2015 amendment. Any remedy must also take into account whether the lost information can be restored or replaced from other sources. *Id.* As discussed above, the information that was lost as a result of defendants' misconduct was important information that could have significantly aided the plaintiff in proving its claims.

As explained above, plaintiff has been irreparably prejudiced by defendants' misconduct. The computer Abbas used to develop CaseGuard from May 2014 until it was destroyed in late 2016 would have answered not only when defendants employed a source code control system in developing CaseGuard, but could have provided direct evidence supporting or undermining plaintiff's claims that CaseGuard was developed from the TraQ Suite 6 source code. By destroying the computer, defendants foreclosed a critical avenue for discovery and greatly harmed plaintiff's ability to prosecute the case. Similarly, the source code control system and thousands of CaseGuard-related files deleted from the replacement computer were relevant to plaintiff's claims and also could have helped establish that CaseGuard was derived from TraQ Suite 6. Due to this permanent destruction of material evidence, plaintiff has been put in the unfortunate position of having to spend significant sums in preparing its case based mainly on circumstantial evidence.

Taking into account defendants' conduct and the Rule 37(e) advisory committee's guidance, the undersigned recommends a finding that as an appropriate remedy the district judge should consider instructing the jury that defendants had a duty to preserve electronically stored information as of May 16, 2016 and that they failed to preserve that material information. The jury should also be instructed that the defendants failed to comply with a court order to provide the plaintiff with information relevant to its claims against the defendants during discovery.

Moreover, given the serious nature of defendants' conduct, the jury should be instructed to presume that the information on the computer used to develop CaseGuard that was destroyed by the defendants in late 2016 and the source code control system that had been on the replacement computer that was destroyed by the defendants in July 2017 would have been unfavorable to the defendants. Without having additional information concerning the analysis of the thousands of CaseGuard-related files that were deleted in July 2017 and whether they could be recovered, it is recommended that the jury be instructed that they could presume that the information contained in those files would have been unfavorable to the defendants. Finally, given that plaintiff seeks an award of attorney's fees and costs for the entire litigation in its complaint, the issue of attorney's fees and costs incurred as a result of defendants' misconduct should be taken under advisement until the conclusion of this action.

Conclusion

For the reasons stated above, the undersigned magistrate judge recommends that plaintiff QueTel Corporation's motion for sanctions (Docket no. 35) be granted in part. The undersigned recommends that the district judge instruct the jury: (1) that they are to presume that the information on the computer used to develop CaseGuard that was destroyed by the defendants in late 2016 and the source code control system that had been on the replacement computer that was destroyed by the defendants in July 2017 would have been unfavorable to the defendants when weighing the evidence whether the defendants misappropriated plaintiff's TraQ Suite 6 source code; (2) that they may presume that the information contained in thousands of CaseGuard-related files that were deleted in July 2017 would have been unfavorable to the defendants when weighing the evidence whether the defendants misappropriated plaintiff's TraQ Suite 6 source code; and (3) that defendants failed to comply with a court order to provide plaintiff with

information relevant to its claims and the plaintiff was not given access to all the computers used by the defendants in developing CaseGuard.

Notice

By means of the court's electronic filing system, the parties are notified that objections to this proposed findings of fact and recommendations must be filed within fourteen (14) days of service of this proposed findings of fact and recommendations and a failure to file timely objections waives appellate review of the substance of the proposed findings of fact and recommendations and waives appellate review of any judgment or decision based on this proposed findings of fact and recommendations.

Entered this 27th day of October, 2017.

/s/
John F. Anderson
United States Magistrate Judge

Alexandria, Virginia

John F. Anderson
United States Magistrate Judge