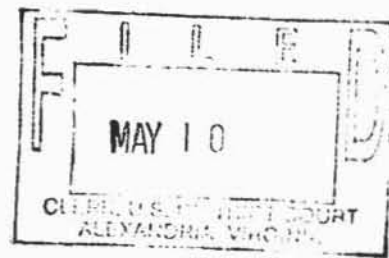


**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division**



ANIMATORS AT LAW, INC.,
Plaintiff,

v.

CAPITAL LEGAL SOLUTIONS, LLC,
et al.,
Defendants.

Case No. 1:10cv1341

ORDER

At issue in this Computer Fraud and Abuse Act ("CFAA")¹ action is whether defendants are entitled to partial summary judgment² with respect to plaintiff's CFAA claim on the ground that plaintiff has failed to demonstrate the requisite jurisdictional "loss" of \$5,000 or more, as required by the statute. *See* 18 U.S.C. § 1030(c)(4)(A)(i)(I).

For the reasons that follow, defendants' motion for partial summary judgment must be denied.

¹ *See* 18 U.S.C. § 1030.

² Plaintiff's complaint asserts thirteen claims for relief, all but one of which are state law claims. Because the parties are not diverse, plaintiff asserts federal jurisdiction based on a claim brought under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. Defendants moved to dismiss the complaint, contending that plaintiff's CFAA claim failed with respect to the jurisdictional loss requirement, and that the remaining state law claims should then be dismissed on jurisdictional grounds. *See Yashenko v. Harrah's NC Casino Co., LLC*, 446 F.3d 541, 553 n.4 (4th Cir. 2006) ("Once a district court has dismissed the federal claims in an action, it maintains 'wide discretion' to dismiss the supplemental state law claims over which it properly has supplemental jurisdiction.") (citation omitted). The motion was denied because plaintiff's complaint was sufficient to state a CFAA claim, but the parties were permitted limited discovery on the issue of the jurisdictional loss requirement to allow consideration of this pivotal issue on a more complete record.

I.³

Animators at Law, Inc. (“Animators”), a Virginia corporation providing litigation support services in graphics and technology, brought this action against three defendants: (i) Capital Legal Solutions, LLC (“CLS”), a Virginia limited liability company also engaged in litigation support services; and two individuals formerly employed by Animators and currently employed by CLS: (ii) April Tishler, and (iii) William Yarnoff. In essence, Animators alleges that beginning in early 2010, CLS conspired with Tishler and Yarnoff, who were then employed by Animators, to leave Animators’ employment to become CLS employees, and to take with them confidential and proprietary information about Animators’ services, projects, and clients.

Tishler and Yarnoff abruptly left Animators’ employment to join CLS on March 9, 2010. On March 17, Ken Lopez, Animators’ president, noticed that an Animators laptop containing sales information was missing. The laptop had been used previously by Tishler, and after emailing Tishler, Lopez learned that the laptop had been retained by Tishler or another former Animators employee working at CLS. Because the laptop was believed to contain Animators’ confidential files, the discovery that it had been in the possession of someone at CLS led Lopez to suspect that Tishler, Yarnoff, or others at CLS may have accessed the files on the computer without authorization.⁴ Thus, Lopez initiated an investigation concerning whether defendants

³ All facts recited here are undisputed unless otherwise stated, and where any disputes of fact are noted, the analysis proceeds by assuming the version of the dispute most favorable to the non-movant—in this case Animators. *See Sapphire Dev., LLC v. Span USA, Inc.*, 120 Fed. Appx. 466, 470 (4th Cir. 2005). Specifically, while defendants dispute that they violated the CFAA, they concede that for the purposes of summary judgment, it is appropriate to take Animators’ version of the unauthorized access as true. Thus, Animators’ version of the events, including the alleged unauthorized access, is reflected in the factual recitation here.

⁴ The parties do not dispute that any access to Animators’ confidential files by Tishler, Yarnoff, or any other former Animators employees after leaving Animators would constitute unauthorized access.

copied, deleted, or otherwise misused Animators' confidential information after leaving Animators' employment.

Lopez, suspecting that an unauthorized intrusion had occurred, directed that the laptop be delivered to Intelligent Discovery Solutions, Inc. ("IDS") for forensic analysis. Lopez also suspected that Tishler and Yarnoff has conspired with CLS to steal confidential information from Animators, and thus requested IDS to analyze its computer system. IDS conducted an examination of the laptop as well as three other items, namely two "spare bundle images"⁵ and a hard drive from an Apple iMac computer, but only the investigation of the laptop was directly related to the unauthorized computer access by Tishler and Yarnoff. IDS was "tasked with trying to identify [any] evidence related to the taking and deletion of Animators at Law proprietary or confidential information." *See* Def. Ex. 3, PL000102.⁶ IDS's "Preliminary Instigative Report" concerning its examination indicated that after Lopez inquired with Tishler about the missing laptop and before the laptop's return to Animators, approximately 800 files and folders were deleted from the laptop. *See* Def. Ex. 3, PL000102-21. According to Lopez, at least twelve of the files contained confidential Animators information.

The parties dispute whether Animators incurred any actual costs for IDS' services, and if so, what costs can be specifically attributed to the laptop analysis. The engagement letter from IDS to Animators provides, in pertinent part, as follows:

[Animators] shall compensate IDS for services provided, which shall include Consultant's fees, support services hourly fees, computer charges, and reimbursable costs and expenses. Consultant's hourly fee is \$00.00. IDS' current

⁵ Although the record is not especially clear on this point, it appears that the spare bundle images appear contain backup files from Animators' computer systems.

⁶ In lieu of page numbers, defendants' summary judgment exhibits contain only Bates numbers, such as "PL000102," These Bates numbers are included where applicable for reference purposes.

hourly staff rates range from \$00.00 per hour [sic] for research analysts, associate and senior associates, and senior professional staff. Hourly rates may change in the future. To expedite prompt payment, IDS may also send copies of its invoices directly to [Animators]

Def, Ex, 3, PL000077-78. IDS did not provide an invoice to Animators until March 10, 2011, six days after the parties were granted leave to conduct limited discovery into the dollar value of Animators' losses. That invoice bills Animators for \$54,210 in charges, which are broken down into two categories. *See* Def. Ex. 3, PL000085. First, the invoice indicates that three IDS consultants cumulatively provided 63.3 hours of "[p]rofessional [s]ervices" at rates ranging from \$200 to \$450 per hour, for a total of \$24,515. *Id.* This invoice is supported by billing logs, in which the consultants detailed how their time was spent down to the tenth of an hour. According to IDS' managing director, a "majority" of this time—which, literally, interpreted, would equate to at least \$12,257.51—was spent working on the laptop. *See* Def. Ex. 3, PL000092. Second, the invoice indicates "[h]osting [s]ervices" totaling \$29,695, which includes charges for hosting and loading data (at \$60 per gigabyte) and other "[u]ser [c]harges." *See* Def. Ex. 3, PL000085. IDS's managing director attributes \$7,243.90 of these costs exclusively to the laptop. In sum, although the parties continue to dispute the precise total cost of these services, the summary judgment record establishes that at IDS provided *at least* \$19,501.41 worth of services exclusively for investigating unauthorized access of the laptop.

Even so, defendants dispute whether this \$19,501.41 qualifies as a CFAA loss, because they contend that Animators did not actually pay IDS for the services. Animators and IDS apparently had a longstanding, ongoing business relationship, where formal invoices and payments were sometimes not exchanged. Although the record is not especially clear as to what services each company provided the other as a part of this relationship, the parties do not dispute that Animators never paid IDS in cash for the laptop analysis. Yet, Animators points out that on

March 7, 2011—albeit more than a year after the laptop analysis was performed—Lopez provided IDS with a discounted subscription to Law Prospector,⁷ a separate service owned by Lopez that provides information about law firms and major cases. Lopez testified in his deposition that he arranged for this subscription as compensation for IDS's services in an effort to get "everything papered"—that is, to collect paperwork concerning Animators' CFAA losses for discovery purposes. *See* Lopez Dep. at 123. Thus, Animators contends that the IDS laptop analysis resulted in a CFAA loss given as Animators obtained IDS' services on credit and in trade for other services, including the Law Prospector subscription. Defendants argue that Animators incurred no financial cost for IDS' laptop services, and that the invoices and the Law Prospector subscription agreement constitute sham paperwork intended to inflate Animators' purported CFAA losses. On this summary judgment record, there is a material factual dispute as to whether the invoices and Law Prospector subscription agreement were shams or rather, as Animators suggests, mere formalizations of an understood agreement between two businesses with an ongoing, essentially barter relationship. Thus, it is appropriate at this stage to adopt Animators' view of the dispute⁸ and to conclude that, for the purposes of the summary judgment analysis, Animators obtained at least \$19,501.41 in IDS services on a credit or trade basis.

In any event, misuse of Animators' laptop is not the only unauthorized computer access at issue in this case. On April 1, 2010, Lopez discovered that Tishler had accessed two internet-based data services used by Animators, namely (i) the company's "Dropbox" account, a file storage account accessible to certain Animators employees and used to store confidential

⁷ The parties' briefs do not disclose the fair market value of the subscription or the amount of the discount.

⁸ *See Sapphire*, 120 Fed. Appx. at 470 (at summary judgment, the analysis should proceed by assuming the version of any dispute of fact most favorable to the non-movant).

information; and (ii) “GetMyTime,” an internet service for tracking employees’ time. Dropbox accounts are accessible both from Animators’ computers and from a remote computer by anyone with an appropriate Dropbox password. Tishler and Yarnoff were provided Dropbox passwords while employed by Animators, and these passwords were not disabled after they resigned. Lopez reviewed Dropbox records and concluded that Tishler and Yarnoff remotely accessed or downloaded confidential files, including employees’ time records, after resigning from Animators. Similarly, Lopez concluded Tishler and Yarnoff viewed, added, downloaded, altered, and/or deleted various time records from GetMyTime after they left Animators’ employment.

After discovering the unauthorized Dropbox and GetMyTime use, Animators replaced Dropbox with another file storage service called “Box.net” starting April 28, 2010. Although the version of the Dropbox service Animators used was free, Lopez concluded that Animators needed a premium Box.net account for \$175 per month. Animators does not provide information further explaining this increase in cost, nor does it cite any facts in the record to indicate why a simple change to the Dropbox passwords would not have remedied the loss attributable to the unauthorized intrusion.

Animators claims two additional sources of loss for CFAA purposes, namely the time spent responding to the alleged intrusion by Lopez and by David Greenspan, Animators’ attorney. Lopez did not keep a precise or contemporaneous log of the hours he spent responding to the unauthorized computer access, but he has provided estimates. In total, Lopez estimates that he spent 72.5 hours of time on these activities, which includes, by way of example, twelve hours in meetings with IDS, twenty hours communicating with Greenspan, and twelve hours setting up the Box.net service. *See* Def. Ex. 3, PL00043. Lopez represents that his “standard

hourly rate” is \$300 per hour, such that the total “cost” of Lopez’s time spent responding to the alleged CFAA violation would be \$21,750.⁹ *See* Lopez Decl. at 1. As to Greenspan, billing logs indicate that Greenspan spent 31.6 hours overseeing the investigation and resecuring of the system following the unauthorized access. Greenspan billed Animators for this time at his normal hourly rate of \$445 per hour, the cost of which was \$14,062. Greenspan’s activities include coordinating the computer forensics investigation of the laptop and assisting Lopez in drafting letters to defendants concerning the unauthorized access. These letters apparently served two purposes, namely (i) obtaining more information from defendants themselves about their accessing Animators’ files, and (ii) obtaining defendants’ voluntary agreement to cease further unauthorized access.

In sum, at a minimum, the undisputed facts on summary judgment reveal, at a minimum,¹⁰ the following figures for costs or losses incurred by Animators in investigating and responding to the unauthorized computer access:

- i. \$19,501.41 in services provided by IDS, which Animators obtained on credit or in trade as part of an ongoing business relationship with IDS;
- ii. \$175 per month for Box.net services since April 28, 2010;
- iii. \$21,750 for time Lopez’s time responding to the alleged CFAA violation; and
- iv. \$14,062 for time Greenspan’s time overseeing the investigation.

It remains to consider whether these costs are qualified CFAA losses.

⁹ This figure represents the internal cost to Animators. Naturally, as President of Animators, Lopez did not actually bill the company for his time.

¹⁰ Other miscellaneous costs identified by Animators are not listed, such as courier services and shipping costs, because the amounts are too trivial to alter the result ultimately reached here, namely that Animators has demonstrated more than \$5,000 of qualified CFAA losses.

II.

The summary judgment standard is too well-settled to require elaboration here. In essence, summary judgment is appropriate under Rule 56, Fed. R. Civ. P., only where, on the basis of undisputed material facts, the moving party is entitled to judgment as a matter of law. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). Importantly, to defeat summary judgment the non-moving party may not rest upon a “mere scintilla” of evidence, but must set forth specific facts showing a genuine issue for trial. *Id.* at 324; *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 252 (1986). Thus, the party with the burden of proof on an issue cannot prevail at summary judgment on that issue unless that party adduces evidence that would be sufficient, if believed, to carry the burden of proof on that issue at trial. *See Celotex*, 477 U.S. at 322.

III.

The sole issue presented by defendants’ motion for partial summary judgment is whether Animators’ has incurred at least \$5,000 worth of qualified losses under the CFAA. It is appropriate to begin the analysis with a brief overview of the CFAA.

The CFAA prohibits, *inter alia*, any person from “intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer.” 18 U.S.C. § 1030(a)(2). In addition to setting forth criminal penalties for violations, the statute provides that “[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator.” § 1030(g). To maintain a civil action under the CFAA, however, a plaintiff must show that the alleged violation “caused . . . loss . . . aggregating at least \$5,000 in value.” 18 U.S.C. § 1030(c)(4)(A)(i).¹¹ The CFAA specifies that a qualifying “loss” under the statute

¹¹ Claims alleging (i) impairment of a medical diagnosis, (ii) physical injury to a person, (iii) a

means any reasonable cost to any victim, including [i] the cost of responding to an offense, [ii] conducting a damage assessment, and [iii] restoring the data, program, system, or information to its condition prior to the offense, and [iv] any revenue lost, cost incurred, or other consequential damages incurred because of the interruption of service[.]

§ 1030(e)(11). Plaintiff's alleged damages must fall within this definition in order to qualify as a "loss" under the CFAA and therefore satisfy the \$ 5,000 jurisdictional minimum. *Id.* And although cases discussing the CFAA provisions are not abundant, it is clear that the statute requires a plaintiff to prove that the losses in issue were reasonable and that they were caused by the CFAA violation. *See Global Policy Ptnrs, LLC v. Yessin*, 686 F. Supp. 2d 642, 647 (E.D. Va. 2010) (holding that a plaintiff seeking to recover "qualifying costs" under the CFAA must show "that the costs are 'reasonable' and that they were 'caused' by a CFAA violation").

The Fourth Circuit in *A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009), considered the types of damages that may qualify as CFAA losses. There, the defendant operated a plagiarism detection service known as "Turnitin," where students submitted papers for their classes online to Turnitin, and papers were automatically compared with other papers to determine the likelihood of plagiarism. In a suit by students against the defendant for copyright infringement, the defendant counterclaimed that one of the plaintiff students violated the CFAA by submitting papers using another student's user name and password. Upon learning that this student had registered and submitted papers on behalf of another, the defendant became concerned that a technical glitch allowed the intrusion to occur and investigated the matter thoroughly, only to discover that the plaintiff student had simply used another student's Turnitin user name and password found on the internet. Although the plaintiff student in issue

threat to public health or safety, or (iv) damage affecting a computer used by the United States Government in furtherance of the administration of justice, national defense, or national security are exempted from the \$ 5,000 requirement. *See* 18 U.S.C. § 1030(c)(4)(A)(i), (g). None of these exemptions apply here.

conceded that his use was unauthorized for CFAA purposes, inasmuch as the conduct violated the Turnitin terms of service, he argued that the defendant's time spent investigating the incident did not qualify as a CFAA loss. The district court agreed, dismissing the counterclaim, but the Fourth Circuit reversed, holding that the definition of "loss" under the CFAA was "broadly worded" and "plainly contemplates . . . costs incurred as part of the response to a CFAA violation, including the investigation of an offense." *Id.* at 645-46. In remanding, the court "express[ed] no opinion as to whether . . . the alleged consequential damages were reasonable, sufficiently proven, or directly causally linked to [the] alleged CFFA violation." *Id.* at 646.

After *iParadigms*, the district court in *Yessin*, 686 F. Supp. 2d 642, further elaborated on the requirements for qualified CFAA losses. The plaintiff in *Yessin* sought three types of damages for defendant's unauthorized access of plaintiff's email accounts and website: (i) expenses for establishing new email addresses and a new website, (ii) lost "billable time" spent investigating and responding to the offense rather than conducting business, and (iii) lost revenue from failing to win a business opportunity. *Id.* at 648. *Yessin* held that "lost revenue damages may qualify as losses under the CFAA when they result from time spent responding to an offense," but further lost revenue or consequential damages—such as the losses associated with a missed business opportunity—are only recoverable if they were "incurred because of interruption of service." *Id.* at 654 (citing § 1030(e)(11); *iParadigms*, 562 F.3d at 646; *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 562 (2d Cir. 2006) ("[T]he plain language of the statute treats lost revenue as a different concept from incurred costs, and permits recovery of the former only where connected to an 'interruption in service.'")). Thus, *Yessin* held that only the first two types of losses identified by the plaintiff in that case—namely (i) expenses for the new

email addresses and website, and (ii) the time spent responding to the offense—were eligible to be considered as losses for CFAA purposes.

Yessin next considered whether the costs incurred by the plaintiff “were reasonably foreseeable” and “reasonably necessary in the circumstances” to restore and resecure the system. 686 F. Supp. 2d at 647-48. After a fact-intensive analysis of the summary judgment record, the court held that the plaintiff had failed to meet her burden to show that the costs incurred for setting up a new website and email addresses were reasonably necessary. Most of the costs identified by plaintiff were duplicative, vague, inflated on their face,¹² or otherwise unrelated to resecuring the computer system. *Id.* at 649. For example, plaintiff cited costs for creating new content and images, even though the old content and images could have been moved from the old website without compromising security. *Id.* at 649-50. Such costs were not recoverable under the CFAA.¹³ Additionally, while the court in *Yessin* recognized that time spent away from ordinary activities to investigate and respond to the alleged CFAA violation may be recoverable under the Act, the plaintiff could not recover the value of her time because the “description of the tasks performed during [the reported fifty hours of time] is so vague that no reasonable jury could conclude that the expended time was reasonably necessary to restore or resecure the system.” *Id.* at 652. After reviewing all of the alleged costs and eliminating those that were vague, unnecessary, or otherwise not recoverable under the CFAA, *Yessin* concluded that the

¹² For example, the court held that while new web hosting services were qualified CFAA losses, the figures were “clearly overstate[d] . . . because they include five years of web hosting service.” The court held that, at most, plaintiff created a triable issue of fact as to one year’s worth of services, and accordingly divided the figure by five to calculate the CFAA qualified loss amount for summary judgment purposes. 686 F. Supp. 2d at 650.

¹³ In essence, *Yessin* recognized that while a CFAA plaintiff could recover the costs of investigating and resecuring a computer system following an intrusion, it would not reimburse a plaintiff for upgrading from a station wagon to a Rolls Royce.

plaintiff had created a triable issue of fact only as to \$2,283.07 in qualified losses. Accordingly, defendant was granted summary judgment on the CFAA claims.

Here, unlike in *Yessin*, the costs reported by Animators create a triable issue of fact as to well over \$5,000 in qualified CFAA losses. Just as in *iParadigms*, where the CFAA claimant believed that its system had been compromised and went to great lengths to investigate the intrusion, so, too, did Animators come to suspect that its confidential information had been accessed without authorization by former employees and accordingly, took action to investigate and respond to the incident.¹⁴ To determine whether unauthorized access in fact occurred and the extent of such access, Animators had the laptop analyzed by IDS. Although defendants contend that such an extensive analysis was neither reasonably foreseeable nor necessary, a reasonable jury might well disagree and conclude otherwise. Indeed, as *iParadigms* teaches, an investigation is often required to determine the cause and scope of a computer intrusion, and the financial impact of even a relatively narrow intrusion can be extensive. In this case, had Animators' confidential information about clients been compromised, Animators might well have had to address the security breach on a client-by-client basis, potentially adversely affecting Animators' business activities. A jury reviewing the facts in the light most favorable to Animators may reasonably conclude that, in light of this risk, Animators acted reasonably in ordering an in-depth investigation complete with forensic analysis of the misappropriated laptop. In the end, Animators' investigation may disclose that no files were compromised, just as the defendant in *iParadigms* eventually learned that its system had never actually been insecure in the first place. Yet, hindsight must not guide such an analysis of whether such actions were reasonably necessary in response to a CFAA violation; instead, as with any reasonableness

¹⁴ Whether the suspicion was reasonable and the actions taken reasonable are appropriate issues for a jury.

inquiry, the analysis should focus on whether reasonable prudence was exercised in light of the risks and circumstances presented. Furthermore, perpetrators of unauthorized access should foresee that their actions may result in significant investigations and costs far exceeding the actual damage to the system. In sum, on this summary judgment record, Animators has created a triable issue of fact as to whether \$19,504.41 worth of IDS services were reasonably necessary or foreseeable in response to the CFAA violation.

Additionally, as previously noted, while defendants are free to argue that Animators did not actually incur \$19,504.41 in costs because they never paid IDS in cash, Animators is correct that the CFAA does not require losses to be paid for in cash. Indeed, a holding that CFAA losses must be reduced to a cash exchange would conflict with the principle that a CFAA plaintiff may recover damages for its own employees' time spent responding to CFAA violations.¹⁵ Moreover, defendants essentially argue that IDS performed \$19,504.41 worth of services for Animators for free, a contention that defies common sense. It would be passing strange for IDS' consultants to spend more than sixty hours of time analyzing Animators' data—at least half of which was attributed directly to analyzing the laptop retained by Tishler—without any expectation of compensation in some form. At a minimum, the summary judgment record provides a triable issue of fact as to whether the services were provided on credit or in trade consistent with an ongoing business relationship between IDS and Animators. Thus, a jury could reasonably conclude that the costs of IDS' services were internalized by Animators and thus qualify as CFAA losses.

¹⁵ See *iParadigms*, 562 F.3d at 646 (quoting with approval *SuccessFactors, Inc. v. Softscape, Inc.*, 544 F. Supp. 2d 975, 980-81 (N.D. Cal. 2008), in which the district court held that the value of "many hours of valuable time away from day-to-day responsibilities" are contemplated within the CFAA's definition of "loss").

In light of this conclusion, it is unnecessary to analyze the remaining costs cited by Animators. Yet, it is worth noting that the time spend by Lopez and Greenspan appear to be qualifying CFAA losses as well. Although Lopez provides estimates of his time, these estimates, unlike those provided in *Yessin*, are corroborated in part by time logs provided by IDS consultants and Greenspan. Additionally, even though Greenspan is an attorney working for Animators, a jury may conclude that hiring an attorney to investigate the intrusion and oversee the investigation was reasonably foreseeable and reasonably necessary under the circumstances. Even Greenspan's work drafting letters to defendants may be deemed appropriate measures for containing the security breach, inasmuch as the letters sought defendants' cooperation in investigating the intrusion and preventing further intrusions. While defendants may contend that Greenspan is not the appropriate person to oversee the investigation and response to the intrusion, given his high hourly rate and legal, rather than technical expertise, even a reduction or outright elimination of Greenspan's charges would still leave Animators with well over \$5,000 in qualified losses. Indeed, the only costs reported by Animators that appear to be insufficiently qualified on this summary judgment record are the costs of switching to Box.net from the free Dropbox service; such a move appears to be an upgrade rather than a reasonably necessary step in resecuring Animators' computer system. In any event, given the holding that IDS' services create a triable issue of fact as to more than \$5,000 of qualified losses, it is unnecessary to consider the remaining losses reported by Animators.


Therefore, because the summary judgment record establishes a genuine issue of material fact as to whether Animators incurred at least \$5,000 of qualified CFAA losses, it is appropriate to deny the motion for partial summary judgment.

Accordingly, and for good cause,

It is hereby **ORDERED** that defendants' motion for partial summary judgment (Doc. No. 38), is **DENIED**.

The Clerk is directed to send a copy of this Order to all counsel of record.

Alexandria, Virginia
May 10, 2011



T. S. Ellis, III
United States District Judge