UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

NEW ENGLAND SYSTEMS, INC. Plaintiff, v. CITIZENS INSURANCE COMPANY OF AMERICA, Defendant.	Case No.: 3:20-cv-01743-SVN MARCH 2, 2022

DEFENDANT CITIZENS INSURANCE COMPANY OF AMERICA'S MEMORANDUM OF LAW IN SUPPORT OF ITS MOTION FOR SUMMARY JUDGMENT

DEFENDANT
CITIZENS INSURANCE
COMPANY OF AMERICA

J. Tyler Butts (ct28641)
Denis J. O'Malley (ct30719)
Robinson & Cole LLP
280 Trumbull Street
Hartford, CT 06103
Telephone: 860-275-8200
Facsimile: 860-275-8299
Email: jbutts@rc.com
domalley@rc.com

ORAL ARGUMENT REQUESTED

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

This insurance coverage dispute between Plaintiff New England Systems, Inc. ("NSI" or "Plaintiff") and its insurer, Defendant Citizens Insurance Company of America ("Citizens"), arises from a June 2019 data breach. The data breach minimally impacted NSI's systems, but spread malware to the computer systems of NSI's clients. NSI claims that it is entitled to insurance coverage for its claimed loss of business income attributable to six of its clients that elected to terminate their relationship with NSI following the data breach. It is not.

For NSI to be entitled to any coverage under Citizens' policy, its usual and regular business activities must have been impaired by the data breach. They were not. In fact, NSI's technicians were able to "immediately" respond to the data breach event and work with NSI's clients to remediate the impacts of the malware on their systems. NSI's work continued unabated despite the data breach. That alone is sufficient to preclude NSI from coverage under the policy, grant Citizens' motion, and enter judgment in Citizens' favor on NSI's remaining claims.

Additionally, and as set forth below, NSI has failed to produce, and is unable to prove at trial, documents or testimony supporting a large portion of its damages calculation – NSI's claimed loss of business income relating to its monthly service contracts for six specific clients. Summary judgment on that portion of NSI's claim is therefore appropriate. Finally, NSI has wholly failed to develop evidence or testimony in support of Count Three – its bad faith claim against Citizens – and summary judgment as to that court is likewise appropriate.

I. RELEVANT FACTUAL BACKGROUND

A. New England Systems, Inc.

NSI is a "managed services provider that provides partially or fully outsourced information technology ('IT') support, IT strategy and consulting, and cybersecurity services." (Citizens' Local Rule 56(a)1 Statement of Undisputed Material Facts ("SUMF"), ¶ 1). At all relevant times, and

specifically in 2019, NSI's focus was on providing outsourced managed IT support for companies of up to 300 employees. (*Id.*, ¶ 2). NSI performed a variety of tasks for its clients, including fixing printers, changing passwords, restoring backups, fixing servers, performing virus scans on machines, installing software patches, helping with emails, addressing malware, helping clients recover from ransomware attacks, and helping clients recover from viruses. (*Id.*, ¶ 3). Put simply, at all relevant times, NSI provided an IT department to companies that did not have their own substantial IT departments. As of June of 2019, NSI had approximately 20 employees. (*Id.*, ¶ 4).

As of June 2019, NSI was made up of three departments: (1) a service department; (2) an accounting department; and (3) a sales department. (*Id.*, ¶ 5). At that time, approximately seventeen employees, the majority of them service technicians, worked in the service department, which provided technical support and service for NSI's clients. (*Id.*, ¶¶ 6-7). The service department primarily relied on two systems to provide service to NSI's clients: (1) ConnectWise, which was the service management system; and (2) Continuum, a cloud-based service which provided NSI's remote monitoring and management tools. (*Id.*, ¶ 8). The service department did not rely on any NSI servers to perform work for NSI's clients. (*Id.*, ¶ 9). Nearly all of NSI's clients needing help would be routed to NSI's helpdesk, which assigned a service technician to the client (*Id.*, ¶ 10).

As of June 2019, there were two employees in NSI's accounting department. (*Id.*, ¶ 11). The accounting department provided accounts receivable, accounts payable, and accounting services to NSI, utilized Microsoft Dynamics, ConnectWise, Microsoft Excel, and email to perform its job functions, and used NSI's hardware and equipment. (*Id.*, ¶¶ 12-13).

Finally, as of June 2019, there were two or three employees in NSI's sales department, which performed account management (including client relationship management) and business

development services. (*Id.*, ¶¶ 14-15). The sales department did not rely on any particular NSI system to perform its duties. (*Id.*, ¶ 16).

NSI offered a variety of IT products and services to its clients, including service agreement contracts (for a term of a certain number of months or years) pursuant to which NSI, in exchange for a monthly fee, would provide its clients with remote and/or onsite IT support. (*Id.*, ¶ 17). The services NSI provided by these agreements could include, by way of example, email management, network management, proactive maintenance, and server support. (*Id.*, ¶ 18). The service agreements also provided that NSI would remediate viruses, ransomware, or malware attacks from its clients' systems. (*Id.*, ¶ 19). These contracts were not limited to a certain number of NSI man-hours, meaning that, if a client had a very large problem that occupied all of NSI's technicians, that client would not be charged extra under the service agreement. (*Id.*, ¶ 20).

All six clients implicated by NSI's claims of lost business income had service contracts with NSI prior to the data breach, and all six clients paid NSI on a monthly basis, at the beginning of the month, for NSI's services. (*Id.*, ¶ 21). In addition to its service contracts, NSI also performed one-off projects for its clients that would not be covered by the service contract, like the purchase and installation of a printer, or the conversion of a client to a new operating system. (*Id.*, ¶ 22).

B. The Data Breach & NSI's Response to the Data Breach

NSI first became aware that it had been impacted by a data breach on June 13, 2019, when multiple clients contacted NSI after noticing that something was encrypted on those clients' servers. (*Id.*, ¶ 23). NSI never undertook forensic review to figure out why or how the event happened, but determined internally that the data breach came through NSI via a security antivirus tool that ran on desktops and through compromised credentials of one of NSI's engineers. (*Id.*, ¶

24). As a result of the data breach, the bad actor(s) were able to access the systems of certain NSI clients and send a virus and malware to those clients, which encrypted the clients' data. (*Id.*, ¶ 25).

Critically, the only NSI system that was impacted by the data breach was the accounting department's Microsoft Dynamics server. (*Id.*, ¶ 26). The data on that server became encrypted, and NSI restored a backup following the breach. (*Id.*, ¶ 27). The fact that the accounting department's Microsoft Dynamics server was encrypted had no impact on NSI's ability to perform services for its clients. (*Id.*, ¶ 28). The data breach did not impact NSI's systems in any way that prevented NSI's technicians from helping NSI's clients. (*Id.*, ¶ 29). In fact, NSI and its technicians took steps to help NSI's clients remedy the data breach-related issues "immediately, as soon as the first call came in…on the evening of the breach." (*Id.*, ¶ 30 (emphasis added)).

NSI elected to perform the necessary virus and malware remediation for its clients itself, rather than involve an outside firm to assist. (*Id.*, ¶ 31).[1] NSI claims that, as a result of that choice, it was unable to perform work for some of its other clients, and that, as a consequence, it lost business income when those relationships ended. At the same time, NSI admits that it continued to perform services under its monthly service agreements for other clients, and that NSI never provided any of its clients with refunds on account of NSI's claimed inability to adequately perform under its various contracts. (*Id.*, ¶ 33).

C. NSI's First-Party Insurance Claim to Citizens

Following the data breach on June 13, 2019, NSI reported the incident to its insurance broker, which notified Citizens. (*Id.*, ¶ 34). NSI's CEO (and 30(b)(6) designee) Thomas McDonald ("Mr. McDonald") spoke with Christopher Guittar ("Mr. Guittar"), the adjuster for Citizens for

[1] NSI never communicated to Citizens that, by electing to assist its clients by itself, NSI was voluntarily electing to not do work for other clients. (*Id.*, ¶ 32).

NSI's first-party claim,[2] on or about June 17, 2019 – just four days after the data breach incident. (*Id.*, ¶ 35). At the time, Mr. McDonald represented to Citizens that there was no direct damage to NSI's systems, and that, at that time, they were not making a claim for first-party damage. (*Id.*, ¶ 36). On June 19, 2019, Mr. Guittar emailed Mr. McDonald to inform him that Citizens was setting up a claim for any potential first-party damage, identified potentially-applicable coverages under the Policy, and requested that Mr. McDonald provide Citizens with certain categories of documentation concerning any claim. (*Id.*, ¶ 37). NSI never sent Citizens a copy of any repair estimate. (*Id.*, ¶ 38). NSI never provided any information to Citizens regarding data loss requiring recovery or reproduction. (*Id.*, ¶ 39). NSI did not forward Citizens a breakdown of damages and costs at the time because, according to Mr. McDonald, NSI was in the process of remediating its clients and the preparation of a damages summary was not a priority. (*Id.*, ¶ 40). In fact, Mr. McDonald could not recall if he sent Mr. Guittar a response to Mr. Guittar's June 19, 2019 email; Citizens' contemporaneous internal claim notes suggest that he did not. (*Id.*, ¶ 41).

On June 27, 2019, Mr. Guittar spoke with Mr. McDonald again to see if NSI was making any first-party claim. (*Id.*, ¶ 42). Mr. McDonald indicated that NSI was not, at that time, making such a claim. (*Id.*, ¶ 43). Following that conversation, Mr. Guittar sent Mr. McDonald a follow-up email echoing his June 19, 2019 email and asking that NSI provide Citizens with relevant documentation to support a first-party claim. (*Id.*, ¶ 44). Mr. McDonald could not recall if he responded to Mr. Guittar's requests for information. (*Id.*, ¶ 45). Again, Citizens' claim file material

[2] In addition to the first-party claim made by NSI against Citizens in this lawsuit, NSI also made a third-party claim to Citizens. That claim concerned NSI's potential tort liability to its clients for damages its clients incurred or sustained as a result of NSI's potential negligence in allowing the data breach to happen. In connection with that claim, Citizens has paid NSI tens of thousands of dollars to protect NSI from lawsuits by its customers and to reimburse its customers for monies spent to recover and restore their systems. That third-party claim is not at issue in this litigation.

suggest that Mr. McDonald did not respond to Mr. Guittar's requests for information at that time. (*Id*., ¶ 46).

Mr. Guittar and Mr. McDonald spoke repeatedly in the following months concerning the data breach and the Policy's first-party coverages, but it was not until December 19, 2019 (more than six months after the data breach) that NSI presented anything approaching a formal first-party claim. (*Id*., ¶ 47). On that date, in a five-page letter sent by its current counsel, NSI demanded that Citizens pay it the full Policy limits of $250,000 for lost business income. (*Id*., ¶ 48). Citizens referred the matter to coverage counsel, who responded to NSI's letter on January 28, 2020 and explained why NSI's claim was not covered. (*Id*., ¶ 49). NSI's counsel responded three months later, on April 20, 2020, disputing Citizens' coverage position and providing, for the first time, documents allegedly supporting NSI's damages claim in the form of proposals and estimates for four of NSI's clients. (*Id*., ¶ 50).[3] Citizens responded to that letter on June 8, 2020, again re-affirming its coverage position. (*Id*., ¶ 53). This litigation followed.

D. Relevant Policy Terms

At all times relevant to this case, Citizens insured NSI under a policy of insurance bearing policy number OBE D918330 00 and with a policy term of May 15, 2019 to May 15, 2020 (the "Policy"). (*Id*., ¶ 54). The Policy includes a Data Breach Coverage Form (the "Form") with an aggregate limit of $250,000 for losses covered by the Form. (*Id*., ¶ 55).[4] It is the terms of this Form,

[3] Notably, none of the proposals provided by NSI's counsel on April 20, 2020 are signed. (*Id*., ¶ 51). More curiously, some were prepared shortly after the data breach. (*Id*.). This means that NSI is seeking to recover business income from allegedly lost projects that were not even quoted, much less agreed-to, until after the data breach. NSI's letter also includes a number of statements that are materially at odds with the testimony of NSI's corporate representative, including that during the 60-day period of indemnity, "NSI had to devote its full attention to restoring its system…" (*Id*., ¶ 52). As Mr. McDonald admitted during his corporate representative deposition, NSI's own systems were minimally impacted by the Data Breach, and NSI's technicians were unimpeded in their efforts to restore their clients' systems immediately following the event. (*Id*., ¶¶ 29-30).

[4] While NSI's claimed damages may exceed this number, the Policy restricts NSI's potential recovery on its breach of contract claim in this case to $250,000.

specifically the "Data Breach Expense Coverage[]" for "Cyber Business Interruption and Extra Expense" (the "Cyber BI Coverage") that NSI claims provide coverage for its claimed losses relating to the data breach. (*Id.*, ¶ 56). That provision provides:

> We will pay actual loss of "business income" and additional "extra expense" incurred by you during the "period of restoration" directly resulting from a "data breach" which is first discovered during the "policy period" and which results in an actual impairment or denial of service of "business operations" during the "policy period".

(*Id.*, ¶ 57 (emphasis added)).

The quoted phrases in the provision set forth above are all defined by the Form. (*Id.*, ¶ 58). "Business income" means, in relevant part, "Net Income (Net Profit or Loss before income taxes) that would have been earned or incurred if there had been no impairment or denial of 'business operations' due to a covered 'data breach'." (*Id.*, ¶ 59 (emphasis added)).[5]

"Period of restoration" for loss of "Business Income" means "[t]he period of time that begins…after 24 hours…immediately following the time the actual impairment or denial of 'business operations' first occurs" and ends on the earlier of " (1) The date 'business operations' are restored, with due diligence and dispatch, to the condition that would have existed had there been no impairment or denial; or (2) Sixty (60) days after the date the actual impairment or denial of 'business operations' first occurs…" (*Id.*, ¶ 60 (emphasis added)).

Finally, "business operations" means NSI's "usual and regular business activities." (*Id.*, ¶ 61).

Taken together, and inputting applicable definitions into the coverage grant of the Cyber BI Coverage under which NSI seeks to recover, the Cyber BI Coverage covers: (1) the actual loss

[5] The definition of "Business Income" also includes "[c]ontinuing normal operating expenses incurred, including payroll," but NSI's calculation of business income does not include this element. Similarly, although "extra expense" may be covered under the Policy, NSI's damages calculation does not include an "Extra Expense" element.

of NSI's net profit or loss before income taxes that NSI would have earned or incurred if there had been no impairment or denial of NSI's usual and regular business activities due to a covered data breach; (2) if the actual loss was incurred by NSI during the period beginning 24 hours immediately following the time the actual impairment or denial of NSI's usual and regular business activities first occurred and ending, at most, sixty days later; and (3) if the actual loss directly resulted from a data breach which resulted in an actual impairment or denial of service of NSI's usual and regular business activities.

Put differently, for NSI to establish entitlement to coverage under the Policy, NSI bears the burden of proving each of the following elements: (1) there was a data breach; (2) that the data breach was first discovered during the Policy period; (3) that the data breach resulted in an actual impairment or denial of service of NSI's usual and regular business activities; (4) that, as a direct result of the data breach, NSI incurred an actual loss of net income that would have been earned if there had been no impairment or denial of NSI's business operations caused by the data breach; and (5) that NSI's actual loss of net income occurred during the period of restoration, as defined by the Policy. The parties do not dispute that elements (1) and (2) have occurred. This motion is focused on element (3). The parties have significant disputes concerning elements (4) and (5) that will be resolved at trial should the case proceed.

E. This Litigation

Following Citizens' denial of its claim, NSI filed this action in October 2020. NSI's Complaint alleged three causes of action against Citizens: (1) Breach of Contract (Count One); (2) Violation of the Connecticut Unfair Insurance Practices Act by and through the Connecticut Unfair Trade Practices Act (Count Two) (the "CUTPA/CUIPA Count"); and (3) Breach of the Covenant of Good Faith and Fair Dealing (Bad Faith) (Count Three) (the "Bad Faith Count"). (*Id.*, ¶ 62).

Citizens removed this matter to federal court in November 2020. (*Id.*, ¶ 63). On December 24, 2020, Citizens moved to dismiss Counts Two and Three of the Complaint. (*Id.*, ¶ 64). On May 17, 2021, Judge Meyer granted Citizens' motion with respect to Count Two – the CUTPA/CUIPA Count – and denied Citizens' motion with respect to Count Three – the Bad Faith Count. (*Id.*, ¶ 65). In permitting NSI to proceed with the Bad Faith Count, Judge Meyer focused on three allegations that, "[t]aken together…are enough for initial pleading purposes to support a claim that Citizens acted in bad faith to impede NSI's rights to the benefits of its insurance policy." (*Id.*, ¶ 66). Those allegations were that:

- "Citizens falsely represented that NSI had waived its right to claim business interruption insurance";
- "Citizens intentionally misrepresented pertinent policy provisions when it allowed NSI to undertake self-repair work without disclosing that Citizens knew it would consider NSI ineligible for business-interruption coverage if it performed such work"; and
- "Citizens engaged in no investigation of its claims whatsoever."

(*Id.*, ¶ 67).

Citizens' Motion for Summary Judgment is directed at the two remaining causes of action in this litigation – Count One (Breach of Contract) and Count Three (the Bad Faith Count).

F. NSI's Claimed Damages

NSI's claim for lost business income in this litigation concerns work that NSI was allegedly unable to perform for six of its clients following the data breach: (1) Albert Brothers, Inc./Cornerstone Realty; (2) Avon Public Library; (3) Community Housing Advocates, Inc.; (4) Star Struck; (5) United Steel; and (6) Wolcott Public Schools. (*Id.*, ¶ 68). NSI's claimed business

income damages can be separated into three distinct categories: (1) cancelled or expired monthly service agreements; (2) cancelled projects; and (3) cancelled or expired subscriptions. (*Id.*, ¶ 69).[6]

First, with respect to cancelled or expired monthly service agreements, NSI claims that, following the data breach, each of the six clients listed above ceased their business relationship with NSI. The precise manner in which each specific business relationship terminated varied depending on the client. For example, NSI claims that Albert Brothers terminated its relationship with NSI in August 2019 with two months remaining on its agreement. (*Id.*, ¶ 70). NSI claims that Avon Public Library terminated its relationship with NSI in November 2019 with twenty-six months remaining on its agreement. (*Id*). NSI claims that Community Housing simply did not renew its contract with NSI when it expired in August 2019. (*Id.*). NSI claims that Wolcott Public Schools similarly elected not to renew its contract with NSI when it expired in August 2019. (*Id.*). NSI claims that Star Struck terminated its relationship with NSI in August 2019 with thirty-two months remaining on its automatically-renewed agreement with NSI. (*Id.*). NSI claims that United Steel terminated its relationship with NSI in April 2020 with twelve months remaining on its agreement. (*Id.*).[7] As a result of the failure of these six business relationships, NSI claims that it is entitled to $627,868.76 from Citizens. (*Id.*). This figure represents NSI's calculation of the gross revenue it would have earned had its clients renewed their contracts and/or maintained their business relationship over the anticipated length of the remaining or anticipated contract, which length ranges from two months (Albert Brothers) to more than two years (Wolcott Public School

[6] The Policy does not treat these three categories differently for purposes of determining whether there is coverage for lost business income. Coverage for the three groups of claimed damages rises and falls as one.

[7] Although NSI claims that each lost client was a direct result of the data breach, testimony by the former clients' corporate representatives revealed a myriad of reasons for leaving, including the choice to bring NSI's job functions in-house, as well as longstanding discontent with NSI's services pre-dating the data breach. However, even if NSI were able to prove that each client's decision to stop its relationship with NSI was solely caused by the fact of the data breach, that does not establish coverage under the Policy. The Policy does not provide coverage for clients that NSI lost as a simple consequence of the data breach itself. NSI's claimed loss of business income must have been actually incurred by NSI as a result of NSI's inability to perform its regular business activities as a result of the data breach.

[twenty-four months], Avon Public Library [twenty-six months], Star Struck [thirty-two months]). (*Id.*).[8]

Second, with respect to cancelled projects, NSI claims that it lost a certain number of projects for United Steel (4 projects), Wolcott Public Schools (3 projects), Albert Brothers (2 projects), and Community Housing (1 project), "which would have been completed" but for the data breach. (*Id.*, ¶ 71). These are projects separate and apart from NSI's obligations to its clients pursuant to its monthly service agreements. NSI claims that it is entitled to a total of $152,024.00 in "estimated income" from these projects that NSI was allegedly unable to perform. (*Id.*).

Third, with respect to cancelled or expired subscriptions, NSI claims that it lost income attributable to fees it charged its clients in connection with the provision of certain subscription services, *i.e.*, Office 365 Advanced Threat Protection, Microsoft Azure, Barracuda cloud services, and NSI Backup TotalCare. (*Id.*, ¶ 72). NSI claims that it is entitled to a "total loss" of $134,162.80 from these subscriptions that NSI's clients elected not to purchase following the data breach. (*Id.*).

All in all, NSI claims that it has suffered $914,055.56 in damage as a result of the data breach. These damages all relate to the claimed loss of just six of NSI's dozens of clients following the data breach with no reference to the global picture of NSI's financial health following the data breach. This is an unusual way of calculating a business income claim. Typically, entities that have suffered a business income loss demonstrate that loss by comparing the business's performance during and after the loss to the business's performance for a similar time frame before the loss. *See, e.g.*, *Hilton v. UK Fragrances, Inc.*, No. 12-CV-6346 JFB AKT, 2014 WL 794304, at *7 (E.D.N.Y. Feb. 25, 2014) (*citing Flexitized, Inc. v. Nat. Flexitized Corp.*, 335 F.2d 774, 779 (2d

[8] The Policy only provides coverage for business income actually lost during the Period of Restoration. NSI's attempt to claim years and years' worth of anticipated future income in this litigation has led to a grossly inflated damages claim in the event there is coverage, which there is not.

Cir. 1964)). As NSI's insurance broker explained to Mr. McDonald in September 2019, "[y]ou would have to compare your income right around the time of loss to one year ago." (SUMF, ¶ 73).

Such an analysis is frequently done by an accountant or other financial professional. NSI has not disclosed an accountant or other expert to perform a business income calculation that takes into account NSI's historical performance, anticipated future performance, market trends, and all of the other factors that may appropriately be considered in determining the true impact of the data breach on NSI's bottom line. However, doing the kind of year-over-year comparison suggested by NSI's insurance broker reveals that NSI suffered little to no loss of business income following the data breach.[9] Comparing NSI's financial performance in 2018 year-over-year to its performance in 2019 (the year of the data breach), NSI's total income (representing NSI's revenue less cost of goods) increased by over $60,000. (*Id.*, ¶ 75). These yearly numbers do not conceal a more limited, monthly, impact of the data breach on NSI's business. Drilling down on a month-over-month basis using NSI's monthly profit and loss statement, and comparing NSI's financial performance from June-August 2018 against June-August 2019, shows an increase in net income.[10]

Instead of providing Citizens with an overarching analysis of NSI's financial health, and the actual impact of the data breach on its business income, NSI has selectively cherry-picked those few, specific, clients for which it happened to experience a loss of work following the data breach. The reason for this selectivity is clear – looking at the bigger picture reveals that NSI suffered little, if any, actual loss of business income in the two months following the data breach, and certainly nothing on the order of the $914,055.56 seeks to recover in this litigation.

[9] Mr. McDonald admitted as much at his deposition, testifying that NSI's income following the Data Breach was "flat, about the same flat from time of the loss from a year ago." (*Id.*, ¶ 74).

[10] NSI's net operating income for those three months in 2018 totaled $52,177. (*Id.*, ¶ 76). For those same three months in 2019, NSI's net operating income totaled $55,935, which is $3,758 higher than the same period of time a year prior. (*Id.*, ¶ 77). A review of NSI's total revenue and gross profit over the three months of June, July, and August yield similar results: NSI's total revenue dropped only $30,479 from 2018 to 2019, and NSI's gross profit was only $3,417 less from 2018 to 2019. (*Id.*, ¶ 78).

II. LEGAL STANDARD

Summary judgment is appropriate "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law". Fed. Rule Civ. Pro. 56. "Summary judgment is properly regarded not as a disfavored procedural shortcut, but rather as an integral part of the Federal Rules as a whole, which are designed 'to secure the just, speedy and inexpensive determination of every action." *Cetotex Corp. v. Catrett*, 477 U.S. 317, 327 (1986). Material facts are only those which "might affect the outcome of the suit." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986). In a motion for summary judgment, the burden is on the moving party to establish that there are no genuine issues of material fact in dispute and that it is entitled to judgment as a matter of law. *Id*. at 256; *White v. ABCO Engineering Corp*., 221 F.3d 293, 300 (2d Cir. 2000). The general rule is that the facts must be viewed in the light most favorable to the party opposing the motion. *Matsushita Electric Industrial Co. Ltd. v. Zenith Radio Corp*., 475 U.S. 574, 587 (1986). Once the moving party has met its burden, the nonmoving party must "set forth specific facts showing that there is a genuine issue for trial," and present such evidence as would allow a jury to find in its favor in order to defeat the motion. *Anderson*, 477 U.S. at 256; *Graham v. Long Island R.R.*, 230 F.3d 34, 38 (2d Cir. 2000). When the moving party has made a showing that the record lacks evidence to support a plaintiff's claim, the plaintiff then has the burden of identifying "specific facts" which create a material issue for trial. *Celotex*, 477 U.S. at 324.

"This remedy that precludes a trial is properly granted only when no rational finder of fact could find in favor of the non-moving party." *Canton v. Mystic Transp., Inc*., 202 F.3d 129, 134 (2d Cir. 2000). "A party opposing summary judgment cannot defeat the motion by relying on the allegations in his pleading, or on conclusory statements, or on mere assertions that affidavits supporting the motion are not credible. At the summary judgment stage of the proceeding,

Plaintiffs are required to present admissible evidence in support of their allegations; allegations alone, without evidence to back them up, are not sufficient." *Censor v. ASC Techs. of Conn., LLC*, 900 F. Supp. 2d 181, 192 (D. Conn. 2012). "Summary judgment cannot be defeated by the presentation . . . of but a 'scintilla of evidence' supporting [a] claim." *Fincher v. Depository Trust & Clearing Corp.*, 604 F.3d 712, 726 (2d Cir. 2010) (*quoting Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 251, 106 S. Ct. 2505 (1986)).

III. ARGUMENT

A. Citizens is Entitled to Summary Judgment on NSI's First Count – Breach of Contract.

(1) NSI Did Not Experience an Actual Impairment or a Denial of Service of its Business Operations.

The Policy's Cyber BI Coverage provides coverage for any actual loss of business income that NSI would have incurred, during the appropriate period of restoration, had there been no impairment or denial of NSI's usual and regular business activities due to the data breach. (*See supra* at I.D.). A plain prerequisite for coverage under the Policy is that there be an actual impairment or denial of service of NSI's regular business activities.

A few examples illustrate the Cyber BI Coverage's potential applicability. Suppose that a department store was impacted by a data breach such that the store's computer systems were rendered inoperable, and the store unable to ring out customers' purchases or take payment. In that case, the Cyber BI Coverage may reimburse the store for the net income it would have expected to earn, but for the data breach's impairment or denial of the store's business operations, during the period of restoration (i.e., for the length of time the store's computers were down, up to sixty days). As another example, suppose that a widget manufacturer was impacted by a data breach that caused the insured's computerized manufacturing equipment to cease milling widgets, causing

the insured to be unable to fill a time-sensitive order for a customer. Again, in that case, the Cyber BI Coverage may reimburse the manufacturer for the net income it would have received had the data breach not ceased its business operations by making its machinery inoperable.

Against that backdrop we have NSI's claim.[11]

The flaw in NSI's claim for Cyber BI Coverage is that NSI's own systems were minimally impacted by the data breach, and none of its systems were impacted in such a way that its technicians could not perform their ordinary job functions. Put simply, the data breach did not cause NSI to experience an "impairment or denial of service of" its "usual and regular business activities."[12] Critically, attending to its clients' virus- and malware-related needs is one of the services that NSI provides to its clients under its monthly service agreements. (SUMF., ¶¶ 3, 19). Those services are a part of NSI's "business operations", i.e., NSI's "usual and regular business activities." (*Id*, ¶ 61). This is why, in the hours following the data breach, NSI's technicians "immediately" set to work assisting its clients and attempting to remove the virus and malware from its clients' systems. (*Id*., ¶ 30). NSI's technicians were able to "immediately" get to work because the data breach did not "impair[]" NSI's ability to provide those services, much less effect a "denial" of those services altogether.

The data breach had no impact on NSI's ability to do what it contracted with its clients to do – respond to those clients' requests for IT assistance to deal with malware or viruses. Mr. McDonald made this abundantly clear in his testimony as NSI's 30(b)(6) witness. Mr. McDonald

[11] There are a plethora of other reasons why NSI's claim for coverage under the Policy fails, including but not limited to: (1) the fact that NSI was performing non-data breach remediation work for its clients in the weeks following the data breach; (2) testimony by NSI's former clients that their reasons for terminating their relationship with NSI was wholly unrelated to the data breach; (3) a near total lack of actually executed contracts or work agreements that NSI now claims it lost the opportunity to perform; and (4) the fact that NSI is only entitled to recover lost business income for the length of the period of restoration. However, given the fact-bound nature of those arguments, they are best reserved for trial.

[12] The one accounting-related system that was impacted by the data breach had no impact on NSI's ability to assist its clients, nor was NSI's ability to perform accounting-related tasks impeded. (SUMF, ¶ 28).

testified that NSI's "accounting systems" were "the only systems impacted" by the data breach. (SUMF Ex. A (NSI 30(b)(6) Depo.), at 93:7-8). Fortunately for the NSI clients affected by the data breach, the impact to NSI's accounting systems had no effect on NSI's ability to service its clients. Mr. McDonald testified that NSI refrained from restoring its accounting systems immediately following the data breach "because we didn't need it to start remediating with the clients. We needed to use all our resources to help our customers. **We didn't need that [the accounting systems] to deliver any of that service**." (*Id*. at 93:22-94:6 (emphasis added)). Mr. McDonald left no ambiguity that NSI's client-facing systems and technicians were fully operational and functioning in the immediate aftermath of the data breach:

> **Q.** Were NSI's techs hindered in any way in their remediation efforts of [NSI's] clients by what happened to the [accounting department's] server?
> **A.** No.
> . . .
> **Q.** . . . So none of [the] systems that the service techs would need to use to help your clients were impacted?
> **A.** Correct.
> . . .
> **Q.** Did the data breach affect NSI's systems in any way that prevented your techs from helping your clients?
> **A.** No, it did not.
> . . .
> **Q.** Okay. So in the time period immediately after the data breach, your techs were working hard to remediate those customers that were impacted by the data breach?
> **A.** Correct.

(*Id*. at 94:7-22, 104:9-12, 175:7-11). Its client-service related equipment having been spared from the data breach altogether, NSI was able to (and did) deploy its technicians to service clients "[i]mmediately, as soon as the first call came in . . . on the evening of the breach." (*Id*., 103:25-104:1). As NSI's technicians were able to spring into action to perform their ordinary business activities "immediately" following the data breach, there was plainly no denial of NSI's business operations, nor any actual impairment of NSI's business operations caused by the data breach.

NSI's problem was not that it was unable to perform its usual business operations of assisting its customers. The problem was that too many of NSI's customers were having issues simultaneously. In other words, if NSI's claims are to be believed, NSI simply had too much work to do. NSI's situation is analogous to the gym membership paradox[13] whereby gyms have many times more members than they can accommodate at any one time. (*Id*. ("Planet Fitness…has, on average, 6,500 members per gym. Most of its gyms can hold around 300 people.")). If all gym members elected to visit a gym at once, the gym would be overwhelmed, even though all of its equipment continued running and operating. Some members might even cancel their agreements or demand refunds, but that does not mean the gym has suffered a loss covered by insurance.

That is what happened here, if NSI's claims are to be believed.[14] NSI's clients paid NSI in the form of monthly service agreements. (SUMF, ¶ 17). Part of the services NSI offered under those agreements was virus and malware remediation. (*Id*., ¶¶ 3, 19). Because many of NSI's clients were impacted by the same event, NSI alleges that it was unable to respond to those clients as quickly as may have been promised under the service agreements. But that is not to say that the data breach impaired the ability of NSI's technicians to service its clients. Rather, the data breach produced a surfeit of work for NSI to do – work which NSI remained entirely capable to and *actually did* perform "immediately" following the data breach. (*Id.*, ¶ 30).

Simply put, NSI failed to structure its business, and its service agreements, in a way that would enable NSI to adequately address its clients' needs in the event of a worse-case scenario wherein some number of its clients needed virus and malware remediation simultaneously. When

[13] "Why We Sign Up For Gym Memberships But Never Go To The Gym", *NPR All Things Considered*, Dec. 30, 2014, *available at:* https://www.npr.org/sections/money/2014/12/30/373996649/why-we-sign-up-for-gym-memberships-but-don-t-go-to-the-gym.

[14] Again, NSI's internal documentation shows NSI provided its clients with non-data breach related services soon after the data breach, calling into question NSI's claims of an extended inability to respond to its customers' needs.

that worse-case scenario happened, NSI claims that it was unable to appropriately respond – not because of the data breach's direct impact on NSI or its systems, but because NSI was overextended, understaffed, and unprepared to respond in the event a critical mass of clients required NSI's contracted-for services at once. While unfortunate for NSI, the Policy does not insure against the consequence of a company's business decisions, nor does it act as a surety or guarantor to protect against the consequences of a company's dissatisfied clients.

Because NSI did not experience an actual impairment or denial of service of its business operations following the data breach, NSI is not entitled to coverage under the Policy's Cyber BI Form, and summary judgment on Count One, in its entirety, is appropriate.

(2) NSI Cannot Establish its Damages for Lost Monthly Service Agreements.

The lion's share of NSI's claimed damages in this action – $627,868.76 of the total amount claimed of $914,055.56 – is related to NSI's claim that it lost the ability to collect revenue from its clients related to its pre-existing monthly service agreements, i.e., the monthly payments made to NSI by its customers in exchange for NSI's services described above. Because NSI has provided no evidence or testimony (expert or otherwise) concerning the appropriate calculation of those damages under the terms of the Policy, summary judgment should be entered in Citizens' favor with respect to that category of NSI's claimed damages.[15]

As set forth above, the Policy provides coverage for the actual loss of "business income" that NSI incurred during the period of restoration. (SUMF, ¶¶ 57, 60). "Business income" is defined to include "Net income (Net Profit or Loss before income taxes) that would have been earned or incurred if there had been no impairment or denial of 'business operations'…" (*Id.*, ¶ 59 (emphasis added)). A company's net income differs from a company's revenue/sales in that the

[15] The Court need not address this argument if it determines that summary judgment as to Count One is appropriate for the reasons set forth *supra* at III.A.(1).

latter simply represents money in the door generated by a company's sale of goods and services, while the former takes into account the expenses and costs of selling those goods or performing those services.[16] At trial, therefore, NSI would be obligated to produce competent evidence concerning the calculation of NSI's net profit or loss before income taxes on each of its monthly service agreements with its clients. That is all it would be entitled to if the Policy were to provide coverage. The Policy, by its plain terms, does not provide coverage for NSI's anticipated gross revenue/sales associated with its service agreements.

Unfortunately, the documents NSI produced in discovery point only to NSI's revenue related to these monthly service agreements, rather than its net income. Put differently, NSI's claim, expressed in its Interrogatory responses, cites only to the face value of the monthly service agreements that NSI allegedly lost. As an example, NSI claims that it had a 12-month contract with Community Housing at a rate of $8,820 a month, and that NSI lost a potential 12-month renewal and that, as a result, NSI is owed $105,840 ($8,820 x 12 months). (SUMF, ¶ 70). But that $105,840 is only NSI's claimed revenue associated with Community Housing's monthly service agreements, rather than NSI's net income from that work. NSI made no effort in its discovery responses to take its revenue figure and calculate NSI's actual net income.

When questioned about NSI's net income for its monthly service agreements, Mr. McDonald indicated that "50% would be our target", meaning that NSI aimed to make, as net income, fifty percent of the face value of the monthly service agreement. (Ex. A, at 59:23-61:8). However, it is clear that figure was simply aspirational, rather than actual. When asked whether

[16] Suzanne Salerno, NSI's Controller, agreed that "revenue minus cost equals net income." (Ex. B (Salerno Depo.), at 34:1-7); *see, e.g., Sturtevant v. Sturtevant*, 146 Conn. 644, 648 (1959) ("In general accounting practice, net income, as applied to this case, would ordinarily consist of total income received by the defendant from all sources, less the legitimate expenses of realizing it, such as office expenses or other expenses of practice"); *Santa Fe Surgery Ctr., LLC v. Sentinel Ins. Co.*, No. 5:19-cv-262-Oc-30PRL, 2020 WL 6018871, at *3 (M.D. Fla. Oct. 7, 2020) ("The plain meaning of 'net income' is 'sales minus cost of goods sold, selling, general and administrative expenses, operating expenses, depreciation, interest, taxes, and other expenses").

NSI was successful in achieving that figure on its monthly service agreements, McDonald indicated that "[s]ometimes we were, sometimes we weren't," and that he "would have to look". (*Id*., at 61:9-16). McDonald stated that NSI's Controller, Suzanne Salerno ("Ms. Salerno"), might know about NSI's net income realization on its monthly service agreements. (*Id*., at 61:17-21).

Ms. Salerno did not know. Ms. Salerno did not know if, at the time of the data breach, NSI had set a desired net income percentage for its service agreements. (Ex. B, at 34:14-16). Ms. Salerno did not know what NSI's net income would be on a typical service agreement. (*Id*., at 34:17-22). In fact, Ms. Salerno, NSI's Controller and the person in charge of NSI's accounts receivable, billing, accounts payable, contract administration, and bank reconciliation, could not identify anyone at NSI who would know. (*Id*., 14:20-15:18; 34:23-24). Separate and apart from NSI's anticipated or expected net income on monthly service agreements generally, neither Ms. Salerno nor Mr. McDonald had taken any steps in connection with this litigation to calculate NSI's historical net income with respect to the six clients that form the backbone of NSI's damages claim. (*Id*., at 35:2-11; Ex. A, at 251:6-253:4).

"It is axiomatic that the burden of proving damages is on the party claiming them.... When damages are claimed they are an essential element of the plaintiff's proof and must be proved with reasonable certainty....Damages are recoverable only to the extent that the evidence affords a sufficient basis for estimating their amount in money with reasonable certainty." *Am. Diamond Exch., Inc. v. Alpert*, 302 Conn. 494, 510 (2011); *see also Ulbrich v. Groth*, 310 Conn. 375, 441–42 (2013). "In order to recover damages, a claimant must present evidence that provides the finder of fact with a reasonable basis upon which to calculate the amount of damages.... [T]he [factfinder] is not allowed to base its award on speculation or guesswork." *Barham v. Wal-Mart Stores, Inc*., No. 3:12-CV-01361 (VAB), 2017 WL 3736702, at *5 (D. Conn. Aug. 30, 2017) (citing *Sir Speedy,*

Inc. v. L & P Graphics, Inc., 957 F.2d 1033, 1038 (2d Cir. 1992)). "A defendant is entitled to summary judgment based on a plaintiff's failure [to] make out a prima facie case for damages only when no reasonable jury could set the amount of damages." *Van Natta v. Great Lakes Reinsurance (UK) SE*, 462 F. Supp. 3d 113, 136 (D. Conn. 2020), *reconsideration denied*, No. 3:18-cv-438 (SRU), 2020 WL 5215461 (D. Conn. Sept. 1, 2020).

"To prove lost profits, a plaintiff must demonstrate both the existence and amount of such damages with reasonable certainty….Although the damages need not be proven with mathematical precision, they must be capable of measurement based upon known reliable factors without undue speculation." *Washington v. Kellwood Co.*, 714 F. App'x 35, 40 (2d Cir. 2017) (citation and internal quotation marks omitted); *Tse v. UBS Fin. Servs., Inc.*, 568 F. Supp. 2d 274, 308 (S.D.N.Y. 2008); *Wang v. Yum! Brands, Inc.*, 2007 WL 1521496, No. 05-CV-1783 (JFB)(MDG), at *6 (E.D.N.Y. May 22, 2007) (precluding plaintiffs from offering evidence of economic damages where "plaintiffs' sole evidence as to the amount of…lost wages [was]…unsubstantiated testimony"). "Evidence is considered speculative when there is no documentation or detail in support of it and when the party relies on subjective opinion." *Am. Diamond Exch., Inc.*, 302 Conn. at 511 (internal quotation marks omitted); *see also id.* at 513-14 (holding trial court erred, and that it is "readily apparent that the evidence presented at trial was wholly inadequate to establish the plaintiff's lost profits with reasonable certainty").

NSI's Interrogatory Responses identify the gross revenue of each monthly service agreement as its claimed damage. (SUMF, ¶ 70; Ex. K, ¶ 5). But NSI is indisputably not entitled to those full amounts under the plain language of the Policy. NSI is unable to point to any competent evidence or testimony concerning its anticipated net income for any of its six monthly service agreements. The only evidence provided during discovery concerning this portion of NSI's

claim is Mr. McDonald's testimony that, as a general principle, NSI attempted to receive or recoup 50% of the total revenue of a service agreement as net income. But this figure is wholly speculative and is unrelated to, and unsupported by, any documentation produced by NSI and, critically, unsupported by NSI's own Controller. NSI has similarly failed to retain or disclose any accounting professional or expert to calculate the appropriate measure of these damages. NSI's failure to explain its speculative net income percentage, let alone provide any documentation demonstrating that this figure is in any way accurate, leaves the jury (and Citizens) with nothing but speculation on which to base any calculation of damages that could (were there coverage) be owed under the Policy for NSI's lost monthly service agreements. For that reason, summary judgment on NSI's claim for loss of business income related to the monthly service agreements is appropriate.

B. Citizens is Entitled to Summary Judgment on NSI's Third Count – Breach of the Covenant of Good Faith and Fair Dealing (Bad Faith).

The Connecticut Supreme Court has recognized that, "[t]o constitute a breach of [the implied covenant of good faith and fair dealing], the acts by which a defendant allegedly impedes the plaintiff's right to receive benefits that he or she reasonably expected to receive under the contract must have been taken in bad faith." *De La Concha of Hartford, Inc. v. Aetna Life Ins. Co.*, 269 Conn. 424, 433 (2004); *Mazzarella v. Amica Mut. Ins. Co.*, 774 F. App'x 14, 17 (2d Cir. 2019). "Bad faith is not simply bad judgment or negligence, but rather it implies the conscious doing of a wrong because of dishonest purpose or moral obliquity. [I]t contemplates a state of mind affirmatively operating with furtive design or ill will." *Hutchinson v. Univ. of Saint Joseph*, No. 3:21-CV-325(RNC), 2022 WL 19339, at *3 (D. Conn. Jan. 3, 2022); *Buckman v. People Express, Inc.*, 205 Conn. 166, 171 (1987). Put slightly differently, "[b]ad faith in general implies both actual or constructive fraud, or a design to mislead or deceive another, or a neglect or refusal to fulfill some duty or some contractual obligation, not prompted by an honest mistake as to one's rights or

duties, but by some interested or sinister motive…Bad faith means more than mere negligence; it involves a dishonest purpose." *Alexandru v. Strong*, 81 Conn. App. 68, 80–81 (2004) (citing *Habetz v. Condon*, 224 Conn. 231, 237-38 (1992)) (emphasis added).

"Allegations of a mere coverage dispute or negligence by an insurer in conducting an investigation will not state a claim for bad faith against an insurer." *Mazzarella*, 774 F. App'x at 17; *see also Martin v. Am. Equity Ins. Co.*, 185 F. Supp. 2d 162, 165 (D. Conn. 2002) (same). "[A] plaintiff cannot recover for bad faith if the insurer denies a claim that is 'fairly debatable,' i.e., if the insurer had some arguably justifiable reason for refusing to pay or terminating the claim." *McCulloch v. Hartford Life & Acc. Ins. Co.*, 363 F. Supp. 2d 169, 177 (D. Conn. 2005), *adhered to on reconsideration sub nom. McCulloch v. Hartford Life & Accident Ins. Co.*, No. 3:01CV1115 (AHN), 2005 WL 8165602 (D. Conn. Sept. 29, 2005).

A plaintiff, "[a]t the summary judgment stage of the proceeding, . . . is required to present admissible evidence in support of [his] allegations; allegations alone, without evidence to back them up, are not sufficient….In other words, a plaintiff opposing summary judgment must produce more than a scintilla of evidence, *i.e.*, the evidence must be sufficient for a jury to properly proceed to find a verdict for the party producing it, upon whom the onus of proof is imposed." *Voccola v. Rooney*, 136 F. Sup. 3d 197, 204-05 (D. Conn. 2015) (citations and internal quotation omitted). NSI cannot present facts sufficient to raise a jury question on its allegations of Citizens' bad faith.

As discussed above, NSI cannot establish that it experienced an actual impairment or denial of service of its business operations. Moreover, and at a bare minimum, Citizens had a good faith basis for disputing coverage. The communications between Mr. Guittar and Mr. McDonald in the aftermath of the claim, followed by the correspondence between the parties' counsel after NSI's formal submission of a first-party claim, establish that Citizens had a justifiable reason for denying

NSI's claim and maintaining its coverage position that the Policy does not provide coverage. The fact that that NSI disagrees with Citizens' "belief that these provisions of the Policy bar coverage does not evince bad faith sufficient to support a breach of the implied duty of good faith and fair dealing, or to otherwise suggest that [Citizens] acted in 'an arbitrary and unfounded' manner." *Kim v. State Farm Fire & Cas. Co.*, No. 3:15-CV-879 (VLB), 2015 WL 6675532, at *4 (D. Conn. Oct. 30, 2015); *Carney v. Allstate Ins. Co.*, No. 3:16-CV-00592 (VLB), 2017 WL 10604021, at *3 (D. Conn. Feb. 14, 2017) (same).

In addition to claiming that Citizens improperly denied NSI's claim, NSI's bad faith claim is also based on allegations of wrongdoing in connection with Citizens' investigation of the claim.[17] As set forth above, Judge Meyer found that three of NSI's allegations, taken together, could support a bad faith claim. (SUMF, ¶ 67). Having completed discovery, NSI cannot establish the truth of one, let alone all three, of these allegations. *First*, NSI's claim that Citizens represented that NSI waived its rights to any claim is simply not borne out by the parties' correspondence. Nowhere in Citizens' counsel's January 28, 2020 and June 8, 2020 correspondence is the word "waive" used, (Ex. G; Ex. I), nor has Citizens asserted a waiver defense in this litigation. Instead, Citizens' correspondence merely highlights the fact that NSI represented to Citizens that it was minimally impacted by the Data Brach and that it had no suspension of operations. (*Id.*). *Second*, NSI has not identified any policy provisions that Citizens allegedly misrepresented. Moreover, the Complaint's allegation that Citizens wrongfully "allowed NSI to undertake self-repair work," is belied by McDonald's testimony in which he stated that he did not recall any specific conversation

[17] Citizens propounded an interrogatory on NSI requesting that NSI identify all facts supporting its claim that Citizens breached the covenant of good faith and fair dealing. (Ex. K, ¶ 9). NSI's response repeated back, nearly verbatim, the broad, unsupported allegations of the Complaint. (*Compare* Ex. K, ¶ 9 *with* Complaint, ¶¶ 55). The fact that, after more than a year of litigation, the most NSI could do to support its bad faith claim is parrot back the allegations of the initial pleading demonstrate the weakness of NSI's claim.

with Citizens regarding NSI's decision to remediate its clients, let alone any recollection of Citizens affirming or ratifying that decision. (Ex. A, at 131:21-135:11). *Third*, NSI's claim that Citizens engaged in no "investigation of its claims whatsoever" is flatly contradicted by the indisputable back-and-forth correspondence between the parties. Citizens contacted NSI immediately following the data breach, repeatedly asked for information, had multiple conversations with NSI, and, when it finally received a claim in December 2020, timely responded and engaged in a discussion of the issue with NSI's counsel. (*See supra* at I.C.).[18] There is simply no evidence that Citizens failed to investigate NSI's claim.

Finally, based on the evidence developed by NSI during this litigation, NSI cannot prove, and no reasonable jury could find, that Citizens acted with the requisite state of mind for a bad faith claim, i.e., interested or sinister motive, or dishonest purpose. *Pride Acquisitions, LLC v. Osagie*, No. 12–cv–639(JCH), 2014 WL 4843688, at *13 (D. Conn. Sept. 29, 2014) ("Although intent is generally an issue for the jury to decide, a plaintiff is not entitled to have a claim go to the jury [on a claim of violation of the implied covenant of good faith and fair dealing] where [its] only support for the intent element is a bare assertion of bad faith."); *Halkiotis v. WMC Mortg. Corp.*, 144 F. Supp. 3d 341, 359 (D. Conn. 2015) (granting summary judgment where plaintiff "[did] nothing more than make a bare assertion that [defendant] acted in bad faith in its dealings with him. Such assertions are insufficient to survive summary judgment"). Accordingly, Citizens is entitled to summary judgment on NSI's Bad Faith Count in Count III of the Complaint.

IV. CONCLUSION

For the foregoing reasons, defendant Citizens Insurance Company of America respectfully requests that its motion for summary judgment be granted, and judgment for Citizens entered.

[18] NSI has not disclosed any expert to opine on the adequacy or propriety of Citizens' claim-handling conduct.

DEFENDANT
CITIZENS INSURANCE
COMPANY OF AMERICA

By: /s/ *J. Tyler Butts*

J. Tyler Butts (ct28641)
Denis J. O'Malley (ct30719)
Robinson & Cole LLP
280 Trumbull Street
Hartford, CT 06103
Telephone: 860-275-8200
Facsimile: 860-275-8299
Email: jbutts@rc.com
domalley@rc.com

CERTIFICATE OF SERVICE

I hereby certify that on March 2, 2022, a copy of the foregoing was filed electronically and served by mail on anyone unable to accept electronic filing. Notice of this filing will be sent by email to all parties by operation of the Court's electronic filing system or by mail on anyone unable to accept electronic filing as indicated on the Notice of Electronic Filing. Parties may access this filing through the Court's CM/ECF System.

By: /s/ *J. Tyler Butts*
J. Tyler Butts