IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

HERITAGE VALLEY HEALTH SYSTEM, INC.,	)	
Plaintiff,	)	
v.	)	2:19-cv-1535-RJC
NUANCE COMMUNICATIONS, INC.	)	
Defendant.	)	

MEMORANDUM OPINION

Robert J. Colville, United States District Judge.

Presently pending before the Court is a Motion to Dismiss for Failure to State a Claim (ECF No. 9) filed on behalf of Defendant Nuance Communications, Inc., (hereinafter, "Nuance"). For the reasons stated herein, the motion will be granted.

I. Procedural and Factual Background

This action was filed on November 27, 2019 with the filing of the Complaint (ECF No. 1, "Compl."), and Defendant filed the now-pending Motion to Dismiss with Brief in Support on December 26, 2019. (ECF Nos. 9, 10). Plaintiff has filed a Brief in Opposition thereto (ECF Nos. 13) to which Defendant has filed a Reply. (ECF No. 18). The parties have also addressed proposed supplemental authority. (ECF Nos. 21, 22). The matter is now ripe for disposition.

We have jurisdiction pursuant to 28 U.S.C. §§ 1332 (a)(1).

Plaintiff's Heritage Valley Health System, Inc. ("Plaintiff" or "Heritage Valley")'s suit arises from damages it sustained when malware from the Russian military-launched "NetPetya" cyber-attack in June 2017 entered its computer network system through a network connection

with Nuance Communications, Inc. Count I alleges negligence, Count II alleges breach of implied in fact contract (in the alternative to Count I), Count III alleges unjust enrichment (in the alternative to Count II). Nuance moves to dismiss all counts pursuant to Fed. R. Civ. P. 12(b)(6).

Broadly speaking, Nuance argues that it cannot be held liable for negligence because it was not a party to the Master System Procurement Agreement, between Plaintiff and Dictaphone Corporation ("Dictaphone") (ECF No. 11-3, hereinafter "2003 Agreement"), by which Plaintiff purchased certain healthcare software and hardware from Dictaphone, a non-party, which was maintained through a private portal-to-portal network. And even if the contractual terms bind it, Nuance argues, the negligence claim should be dismissed on the basis of the gist of the action doctrine. Plaintiff alleges since Nuance subsequently acquired Dictaphone and maintained it as a wholly-owned subsidiary, Nuance is liable for any contractual obligations and tort liability arising from Plaintiff's use of the products acquired from Dictaphone, and Nuance should be held liable for poor security practices and governance oversight as it had a broader duty to prevent the cyberattack.

The allegations in the complaint are as follows. Plaintiff Heritage Valley is a Pennsylvania non-profit corporation with its principal place of business in Beaver, Pennsylvania. Heritage Valley provides comprehensive health care for residents of Allegheny, Beaver, Butler and Lawrence counties in Pennsylvania, eastern Ohio, and the panhandle of West Virginia. Compl. ¶ 6. Defendant Nuance Communications, Inc. is a Delaware for-profit corporation with its principal place of business in Burlington, Massachusetts. Compl. ¶ 7.

On June 27, 2017, a malware attack known as the NotPetya malware attack was directed at the Ukraine. Compl. ¶ 12. It is believed the attack was initiated by a group of actors associated with the Russian government. Compl. ¶ 10. The malware was distributed through M.E.Doc, a

Ukrainian tax-filing program. M.E.Doc is a popular service in the Ukraine, similar to TurboTax or Quicken in this country. When M.E.Doc installed a software update on user systems it also downloaded the malware. Compl. ¶ 11. Numerous other cyberattacks occurred in the Ukraine in the years leading up to the NotPetya malware attack, and thus, not only by June 2017 but also well before companies doing business in the Ukraine knew or should have known that the potential for cyberattacks directed at businesses in the Ukraine was very much a real threat. Compl. ¶¶ 12-16.

Plaintiff further alleges the following with respect to Nuance's international expansion. Nuance proclaims itself to be a "leading provider of voice recognition and natural language understanding solutions." Nuance's "solutions and technologies are used in the healthcare, mobile, consumer, enterprise customer service, and imaging markets." Compl. ¶ 17. Specific to healthcare, Nuance offers several distinct product, including medical documentation transcription services and Dragon Medical, which is a dictation software for use by physicians. Compl. ¶ 18. According to a June 2017 fact sheet, the company's healthcare solutions were deployed in 86 percent of all United States hospitals and more than 500,000 clinicians and 10,000 healthcare facilities worldwide used the company's clinical documentation solutions. Compl. ¶ 19.

The Complaint further alleges that throughout the course of its history Nuance has built itself through acquisition. Since 2006 alone the company has made more than fifty different corporate acquisitions. Compl. ¶ 20. As a result of these and other acquisitions Nuance now has more than 150 corporate subsidiaries. More than half of these subsidiaries are headquartered internationally. Compl. ¶ 21. As Nuance boasts on its website: "With more than half of the organization residing outside of the US and a sales presence in more than 70 countries, Nuance

can deliver solutions to numerous local markets and bring global perspective and capabilities to its solutions." Compl. ¶ 22. Part of Nuance's global expansion has included doing business in the Ukraine. Compl. ¶¶ 23-25.

Part of Nuance's international growth has also included expanding its business operations into India, with nine separate subsidiaries incorporated in India and office locations in Karnataka, Haryana, Maharastra, and Uttar Pradesh. Compl. ¶ 26. In February 2017, just months before the NotPetya malware attack, Nuance acquired yet another company headquartered in India, named mCarbon. The acquisition closed in June 2017, just weeks before the NotPetya malware attack. Compl. ¶ 27.

Around 7 a.m. on June 27, 2017, Satish Maripuri, the Executive Vice President and General Manager of Nuance's HealthCare Division, was driving to work when a colleague texted him that "an incident of abnormal nature" was gripping Nuance's computer networks. Compl. ¶ 28. Ten minutes later Maripuri received another text, stating that whatever was happening at the company was "a little more nefarious" than normal. Compl. ¶¶ 29, 30. The NotPetya malware attack affected 14,800 Nuance servers of which 7,600 had to be replaced. The malware attack also affected 26,000 computer workstations of which 9,000 had to be replaced. Compl. ¶ 31. At some point on the morning of June 27, 2017as the malware continued to spread through the company's systems, Nuance was forced to take its client-facing software solutions offline in a belated attempt to stop the malware from spreading to its customers. One client-facing software solution taken offline was iChart, which hosts an application called Dictaphone. Compl. ¶ 32.

Plaintiff alleges that the attack's success with respect to Nuance was a result of poor "security practices and governance oversight." It alleges Nuance became a victim of the NotPetya malware attack as a result of its own information security failings. The sheer number of

Nuance's corporate acquisitions and the reach and pace of its global expansion combined to make meaningful integration of acquired systems and meaningful segmentation of Nuance's growing global network difficult. Moreover, rather than expend the resources necessary to meet this growing cybersecurity risk, Nuance instead did not have or invest in the budget or management that would have been required to adequately address this issue. Compl. ¶ 34. The combination of building the business through corporate acquisition, a drive toward global expansion, and significant corporate debt created a perfect storm of integration mismanagement which in turn created substantial cybersecurity risk. With each acquisition and international expansion Nuance exposed itself and its customers to increasing cybersecurity risk, all the while Nuance did not have the management or funding in place to sufficiently protect against these risks. Compl. ¶¶ 35, 36. These business practices combined to make Nuance unprotected against an eminently foreseeable cyberattack. Compl. ¶ 37.

Ultimately, Nuance's business connections in the Ukraine and negligent information security practices became a conduit for the NotPetya malware to affect the United States healthcare system, including Heritage Valley. Compl. ¶ 40. At approximately 7:30 a.m. on Tuesday, June 27, 2017, Heritage Valley became a victim of the NotPetya malware attack. Compl. ¶ 41. As with Nuance the outbreak ultimately affected a majority of Heritage Valley's servers and workstations by encrypting the file system and files, making the operating systems unbootable and the files contained on the drives inaccessible. Compl. ¶ 42. A forensics analysis from two independent data sources showed that the malware entered Heritage Valley's computer network systems through a trusted virtual private network connection with Nuance. Compl. ¶ 43. The first source was security event logs recovered from a compromised host at Heritage Valley containing the user account credentials the malware used to spread ("the flight path or flight

recording" of the malware). Compl. ¶ 44. The first compromised account found on the logs belonged to an unidentified domain either interconnected to Nuance or had an established trust relationship with Nuance. Compl. ¶ 45. The second credential belonged to the Nuance domain with the userservice account belonging to a senior system engineer at Nuance Communications, located in India. Compl. ¶ 46. The third and fourth credentials belonged to the HCE domain, the domain name of a Nuance business area called Nuance Healthcare. The third compromised account belonged to a Senior Project Manager at Nuance Communications in Massachusetts. Compl. ¶ 47. The fourth compromised user-service account from the Nuance Healthcare domain belonged to a Principal Development Engineer at Nuance Communications in India. Compl. ¶ 48.

The fifth Nuance credential belonged to the iChart domain with the userservice account "ntservice." It is alleged that as pertains to Heritage Valley, this connection is related to an agreement the health system had entered into with Dictaphone Corporation in 2003. Under the agreement, Dictaphone was provided through a trusted point-to-point virtual private network connection known as iChart. Nuance subsequently acquired Dictaphone in 2006. Compl. ¶ 49.

Finally, the sixth and seventh credentials identified were part of Heritage Valley's domain: TMCNET\eetapps and TMCNET\d5h5adm. The eetapps account was the first Heritage Valley account exploited by the NotPetya malware. Compl. ¶ 50.

Thus, based on the malware's flightpath as shown above, a forensics analysis showed that the NotPetya malware entered into Heritage Valley's network systems through Nuance, which in turn had been initially infected by the malware through a connection to a computer user located in the Ukraine. Compl. ¶ 51. This conclusion is consistent with Nuance's own public statements

regarding the malware attack. In particular, Nuance has admitted that its systems became infected through a "trusted development partner" based in the Ukraine. Compl. ¶ 52.

A second forensics data source also supported the conclusion that Heritage Valley became infected with the NotPetya malware through Nuance. Specifically, Heritage Valley's firewall logs showed traffic indicative of the NotPetya malware originating from the virtual private network connection between Nuance and Heritage Valley during the first activity by the malware in Heritage Valley's network. Compl. ¶ 53. The firewall logs showed that at 7:23:44 AM EDT on June 27, 2017, the Nuance virtual private network connected to port 445 of a Heritage Valley server. This server was later determined to be the initial introduction of the malware into the Heritage Valley environment, through the installation and execution of PSEXESVC (PSExec service) on the server. Compl. ¶ 54.

The NotPetya malware affected Heritage Valley's entire health system including satellite and community locations. Compl. ¶ 55. The malware affected every aspect of the health system's ability to operate. Physicians and nurses were forced to re-draw pre-operative laboratory results, laboratories and x-ray machines were down and some patients had to be diverted to other locations. Compl. ¶ 56. Laboratory and diagnostic services at Heritage Valley medical neighborhoods and community locations were closed for days, and acute, ambulatory and ancillary care services impacted for nearly a week. Compl. ¶ 58. Heritage Valley alleges it suffered millions of dollars in damages as a result of Nuance's negligence, including business income loss and costs of repair and restoration of computer network systems, employee overtime and compensation, professional and third-party fees incurred in connection with responding to and remediating the incident, and intangible economic harm including the loss of goodwill. Compl. ¶ 59.

We take judicial notice, pursuant to Fed. R. Evid. 201, of the Press release from the White House Office of Communications, Statement from the Press Secretary dated February 15, 2018, , https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ which states:

> In June 2017, the Russian military launched the most destructive and costly cyber-attack in history.
> The attack, dubbed "NotPetya," quickly spread worldwide, causing billions of dollars in damage across Europe, Asia, and the Americas. It was part of the Kremlin's ongoing effort to destabilize Ukraine and demonstrates ever more clearly Russia's involvement in the ongoing conflict. This was also a reckless and indiscriminate cyber-attack that will be met with international consequences.

II. Standard of Review

A motion to dismiss filed pursuant to Federal Rule of Civil Procedure 12(b)(6) tests the legal sufficiency of the complaint. Kost v. Kozakiewicz, 1 F.3d 176, 183 (3d Cir. 1993). In deciding a motion to dismiss, the court is not opining on whether the plaintiff will likely prevail on the merits; rather, when considering a motion to dismiss, the court accepts as true all well-pled factual allegations in the complaint and views them in a light most favorable to the plaintiff. U.S. Express Lines Ltd. v. Higgins, 281 F.3d 383, 388 (3d Cir. 2002). While a complaint does not need detailed factual allegations to survive a Rule 12(b)(6) motion to dismiss, a complaint must provide more than labels and conclusions. Bell Atlantic Corp. v. Twombly, 550 U.S. 544, 555 (2007). A "formulaic recitation of the elements of a cause of action will not do." Id. (citing Papasan v. Allain, 478 U.S. 265, 286 (1986)). "Factual allegations must be enough to raise a right to relief above the speculative level" and "sufficient to state a claim for relief that is plausible on its face." Id. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (citing Twombly, 550 U.S. at

556). The plausibility standard is not akin to a "probability requirement," but it asks for more than a sheer possibility that a defendant has acted unlawfully.... Where a complaint pleads facts that are "merely consistent with" a defendant's liability, it "stops short of the line between possibility and plausibility of 'entitlement to relief.'" Id. (quoting Twombly, 550 U.S. at 556) (internal citations omitted).

The United States Court of Appeals for the Third Circuit instructs that "a court reviewing the sufficiency of a complaint must take three steps." Connelly v. Lane Constr, Corp., 809 F.3d 780 (3d Cir. 2016). The court explained:

> First, it must "tak[e] note of the elements [the] plaintiff must plead to state a claim." Iqbal, 556 U.S. at 675. Second, it should identify allegations that, "because they are no more than conclusions, are not entitled to the assumption of truth." Id. at 679. See also Burtch v. Milberg Factors, Inc., 662 F.3d 212, 224 (3d Cir. 2011) ("Mere restatements of the elements of a claim are not entitled to the assumption of truth." (citation and editorial marks omitted)). Finally, "[w]hen there are well-pleaded factual allegations, [the] court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief." Iqbal, 556 U.S. at 679.

809 F.3d at 876-77. "Determining whether a complaint states a plausible claim for relief will ... be a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." Iqbal, 556 U.S. at 679 (internal citations omitted)

While a District Court is generally limited to a plaintiff's complaint in assessing a motion to dismiss, when a document is "integral to or explicitly relied upon in the complaint [, it] may be considered without converting the motion [to dismiss] into one for summary judgment." In re Burlington Coat Factory Sec. Litig., 114 F.3d 1410, 1426 (3d Cir.1997) (internal quotations omitted). In addition to considering the allegations of the complaint, in connection with a 12(b)(6) motion, the court may consider matters of public record. Schmidt v. Skolas, 770 F.3d

241, 249 (3d Cir. 2014) (quoting Pension Benefit Guar. Corp. v. White Consol. Indus., Inc., 998 F.2d 1192, 1196 (3d Cir. 1993)).

III. Discussion

A central issue to the resolution of the pending motion is the legal impact, if any of the the 2003 Agreement between Heritage Valley and Dictaphone, despite the fact that Plaintiff brings no claim for breach of that contract.[1] (ECF No. 11-3, hereinafter the "2003 Agreement"). The 2003 Agreement provides that Plaintiff agreed to purchase medical dictation software products for use in its various healthcare facilities from Dictaphone, and Dictaphone agreed to provide software licenses, equipment and installation services. 2003 Agreement § 1.1. Plaintiff also elected to participate in the optional Maintenance Plan, the terms of which are incorporated in the 2003 Agreement. 2003 Agreement § 6.4.

Plaintiff's Complaint acknowledges Nuance acquired Dictaphone[2] when it references "Dictaphone was provided to Heritage Valley through a trusted point-to-point virtual private network connection known as iChart. Comp. ¶ 69. Plaintiff alleges Nuance acquired Dictaphone in 2006 and at some point thereafter became the "owner" of Dictphone's private network connection that was the subject of the 2003 Agreement. Compl. at ¶¶ 1,49.

Plaintiff concedes that Nuance is not a party to the 2003 Agreement, but argues Nuance can be held liable by virtue of Nuance's parent-subsidiary relationship with Dictaphone. Compl. ¶¶ 64, 70. It casts its claims as follows: "the 2003 Agreement only forms a part of the necessary

[1] It is appropriate for the Court to consider the agreement in deciding the motion to dismiss. Plaintiff's Complaint references the 2003 Agreement numerous times, Comp. ¶¶ 69, 71. Nuance attached it to its motion, and in response, Plaintiff attached the Addendum to the 2003 Agreement to its Brief in Opposition (ECF No. 13-1).

[2] Defendant explains that it is a matter of public record - and Plaintiff does not dispute thisi n its brief - that at the time of the 2017 Russian attack, Dictaphone was wholly-owned by Consolidated Mobile Corporation, which was wholly-owned by Nuance. (Dictaphone later merged with Consolidated Mobile Corporation, and was owned by Cerence, Inc. and its wholly-owned subsidiaries. Cerence is a separate, publicly traded company, not part of Nuance). (ECF No. 10 at 5).

background for Heritage Valley's claims, because it establishes how the parties came to have any relationship in the first instance, and more particularly how a malware attack that began in the Ukraine could ever find its way into the computer network systems of a health care provider located in western Pennsylvania." ECF No. 13 at 14.

Should it to be determined that Nuance is bound by the terms of the 2003 Agreement, Nuance argues that agreement only warrants against viruses from Dictaphone programs for a period of 90 days, places the burden of protecting the network from viruses on Plaintiff, and Dictaphone was not to provide any maintenance, support or other assistance to Plaintiff for problems necessitated by damages to Dictaphone software from any external source including computer hackers and acts of war. The 2003 Agreement also includes force majeure and limitation of liability clauses. 2003 Agreement at § 6.2.

Sections 6.1.2 and 6.1.6 of the 2003 Agreement warrant against viruses from Dictaphone programs for a period of 90 days; the agreement was executed on August 29, 2003. They read as follows:

> 6.1.2 Programs Warranty. Dictaphone warrants, for the benefit of Customer only (and subject to the limitations of any Third Party Software warranties), that at the time Customer's license of the Programs commences, and for a period or ninety (90) days thereafter (the "Initial Program Warranty Period"), that the Programs shall conform in all material respects to the Documentation. and that upon delivery by Dictaphone, the Programs will be free of viruses, bugs or contaminants which may cause damage to Customer's systems or interrupt Customer's utilization of the Products.
>
> 6.1.6 Disclaimer. With the sole exception of the warranties set forth herein and to the greatest extent allowed by law, DICTAPHONE DISCLAIMS ANY AND ALL PROMISES, REPRESENTATIONS, AND WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE PRODUCTS (INCLUDING THE EQUIPMENT, THE THIRD PARTY SOFTWARE, AND THE DICTAPHONE PROGRAMS) INCLUDING ITS CONDITION, THE EXISTENCE OF ANY LATENT OR PATENT DEFECTS, AND ITS MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR USE. DICTAPHONE FURTHER DISCLAIMS ANY AND ALL PROMISES,

> REPRESENTATIONS, AND WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE NATURE AND QUALITY OF ANY OTIIER PERFORMANCE BY DICTAPHONE HEREUNDER.

Furthermore, Dictaphone's sole liability is to "at Dictaphone's option, either….re-perform any defective support service or… replace any defective part." Id. at § 8(a).

The Maintenance Agreement has similar protections from liability which arguably bar any claim under the contract.[3] ECF No. 11.-3. It provides at ¶ 4(g) of the Maintenance Plan that:

> 4. SUPPORT LIMITATIONS
>
> No maintenance, support or other assistance will be provided under this Maintenance Agreement for problems necessitated by one or more of the following conditions or causes:
> . . .
> (g) Damage to Dictaphone Programs and Hardware from any external source such as, but not limited to, computer viruses unattributable to Dictaphone, computer hackers, fire flood lightning, earthquake, natural disaster, riots, acts of war, radiation, or nuclear event.

(emphasis added).

The force majeure clause found at § 6.3 states:

> 6.3. Force Majeure. Dictaphone shall not be responsible for delays or failures in its performance resulting from acts or omissions beyond its control or from any events, acts or omissions attributable to any third party manufacturer of the Equipment or Third Party Software, any vendor of Equipment with Dictaphone, the licensor of the Third Party Software to Dictaphone, or any maintenance vendors.

(emphasis added).[4]

[3] Section 1.8 of the Maintenance Agreement provides that "[Plaintiff] is responsible for protecting [its] network environment from viruses and damages resulting from virus infection. [Plaintiff] is also responsible for ensuring virus definition updates are performed consistent with [Plaintiff's] internal virus protection policies. [Plaintiff] is responsible for maintaining any subscriptions necessary to obtain virus updates. Customers who chose to implement anti-virus software other than the approved solution do so at their own risk." ECF No. 11-3 at 23.

[4] As such, a cyber-attack launched by the Russian government which affected many other companies and organizations worldwide -- was arguably beyond Nuance's reasonable control.

Furthermore, at Plaintiff's urging, we note that the 2003 Agreement includes a Business Associate Addendum, which addresses the topic of the use of and disclosure of Protected Health Information under HIPAA. (ECF No. 13-1). The protection of health information is not at issue in this lawsuit. The Business Associate Addendum contains promises regarding data security, and no limitation of liability provision, no disclaimer of warranties, and no force majeure clause. See also id. at § 2(m) (providing that the Business Associate "must comply with all applicable HIPAA security requirements").

To succeed in a negligence action, a plaintiff "must establish the defendant owed a duty of care to the plaintiff, that duty was breached, the breach resulted in the plaintiff's injury, and the plaintiff suffered an actual loss or damages." Merlini ex rel. Merlini v. Gallitzin Water Auth., 980 A.2d 502, 506 (Pa. 2009) (citing Martin v. Evans, 551 Pa. 496, 711 A.2d 458, 461 (1998)).

At Count I, Plaintiff alleges Nuance engaged in affirmative conduct of "implementing a business strategy focused predominantly on international growth," "exposed the computer networks of its customers and the customers of its subsidiaries to an unreasonable and foreseeable risk of harm," specifically, "the persistent threat of cyberattacks whether through malware or otherwise." Compl. ¶ 63. Heritage Valley alleges that this affirmative conduct "imposed a duty on Nuance to exercise reasonable care to ensure that Nuance's computer networks were sufficiently protected against cyber intrusions," particularly given that Nuance's computer networks "maintained trusted connections with third-party entities, including plaintiff Heritage Valley." Compl. ¶ 64. Heritage Valley alleges that Nuance breached this duty "by failing to take proper precautions to protect its computer network systems against the threat of malicious intrusion," thereby causing Heritage Valley "to become a victim of the NotPetya

malware attack," which in turn caused the health system to suffer "substantial damages." Compl. ¶¶ 65-67.

A. Gist of Action

Defendant argues the negligence claim at Count I must be dismissed under the gist of the action doctrine. The "gist of the action" doctrine "is designed to maintain the conceptual distinction between breach of contract claims and tort claims [by] preclud[ing] plaintiffs from recasting ordinary breach of contract claims into tort claims." eToll, Inc. v. Elias/Savion Advertising, Inc., 811 A.2d 10, 14 (Pa. Super. 2002). The simple existence of a contractual relationship between two parties does not preclude one party from bringing a tort claim against the other. Smith v. Lincoln Benefit Life Co., No. 08-1324, 2009 WL 789900, at *20 (W.D. Pa. Mar. 23, 2009), aff'd, 395 F. App'x. 821 (3d Cir. 2010). The doctrine, however, forecloses a party's pursuit of a tort action for the mere breach of contractual duties, "without any separate or independent event giving rise to the tort." Smith, 2009 WL 789900, at *20 (quoting Air Prods. and Chems., Inc. v. Eaton Metal Prods. Co., 256 F. Supp.2d 329, 340 (E.D. Pa. 2003)).

In Canters Deli Las Vegas, LLC v. FreedomPay, Inc., No. CV 19-3030, 2020 WL 2494701, at *10 (E.D. Pa. May 14, 2020) the court explained as follows. Determining whether the gist of the action doctrine applies "call[s] for a fact-intensive judgment as to the true nature of a claim." Williams v. Hilton Grp., PLC, 93 F. App'x 384, 386 (3d Cir. 2004); see also Milo, LLC v. Procaccino, No. 16-5759, 2020 WL 1853499, at *7 (E.D. Pa. 2020). "In this regard, the substance of the allegations comprising a claim in a plaintiff's complaint are of paramount importance, and, thus, the mere labeling by the plaintiff of a claim as being in tort ... is not controlling." Bruno v. Erie, 630 Pa. 79, 106 A.3d 48, 68 (2014). Rather, "[t]o evaluate whether the gist of the action doctrine applies, a court must identify the duty breached, because 'the

nature of the duty alleged to have been breached ... [is] the critical determinative factor in determining whether the claim is truly one in tort, or for breach of contract.'" Downs v. Andrews, 639 F. App'x 816, 819 (3d Cir. 2016) (quoting Bruno, 106 A.3d at 68). "If the facts of a particular claim establish that the duty breached is one created by the parties by the terms of their contract—i.e., a specific promise to do something that a party would not ordinarily have been obligated to do but for the existence of the contract—then the claim should be treated as one for breach of contract." Bruno, 106 A.3d at 68. "If, however, the facts establish that the claim involves the defendant's violation of a broader social duty owed to all individuals, which is imposed by the law of torts and, hence, exists regardless of the contract, then it must be regarded as a tort." Id. The Canters Deli court granted the motion to dismiss as to the negligence claims against defendant on the grounds plaintiffs' negligence claim was clearly barred by the gist of the action doctrine.

A fair reading of the Complaint leads us to conclude that the duty at issue exists only by way of the 2003 Agreement and thus, Heritage Valley's tort claim is barred by the gist of the action doctrine. Without this contract, Defendant would not have an obligation to provide these services at all, let alone an obligation to exercise reasonable care in providing them.

The complaint alleges Nuance continued to provide Plaintiff the same private network connection that was the subject of Plaintiff's 2003 contract with Dictaphone, and in essence, Nuance subsequently breached its contractual obligation by providing Plaintiff a vulnerable-to-attack private network connection in June 2017. Plaintiff argues that the Complaint alleges Nuance breached a broader social duty –arising outside the contract -- owed to all individuals, citing Dittman v UPMC, 196 A.3d 1054 (Pa. 2018), which held that, "in collecting and storing [defendant's employees'] data on its computer systems, [defendant] owed Employees a duty to

exercise reasonable care to protect them against an unreasonable risk of harm arising out of that act." Dittman, 196 A.3d at 1047. The Pennsylvania Supreme Court held the gist of the action did not apply because the hospital's duty to protect its employees' personal information did not stem from a contract to provide data security between the parties but rather from the hospital's affirmative act of collecting employee data as a condition of employment which "exist[ed] independently from any contractual obligations between the parties." Id. at 1054.

The present case is distinguishable from Dittman. In the present case, the parties (Heritage Valley and Dictaphone) entered into a contract which included an express provision of a secure private network connection. Plaintiff alleges that in June of 2017, the date of the cyber attack, Nuance was providing Plaintiff with the same private network connection that was the subject of the 2003 agreement with Dictaphone, and that Nuance provided this to "third-party" "customers of its subsidiary" in exchange for the "benefits of the agreement." Presumably this refers to payments Plaintiff made to Dictaphone for the years following the 2003 Agreement, which Nuance allegedly "commingled with its own revenues." Complaint ¶¶ 63, 64, 72, 73, 76, 77.

Contrary to plaintiffs' arguments, no broader social duty exits for Defendant to provide a secure private network connection for the transmission of Dictaphone software. Plaintiff has alleged an affirmative act in the form of Nuance's implementation of an "acquisition-driven business strategy." The allegations that Nuance owed Heritage Valley a duty to make "good business decisions" and that Nuance breached that duty by implementing a bad business strategy that invested resources on corporate acquisition instead of cyber security is not sufficient to support a claim. Plaintiff has not presented adequate factual averments demonstrating that Nuanced breached any social duty beyond the obligations of the contract. See The Knit With v.

Knitting Fever, Inc., 2009 WL 3427054 (E.D. Pa. Oct. 20, 2009) (tort claims dismissed under gist of action doctrine as defendant had no broad social duty to provide yarn it represents to be of a certain quality absent a contract). Thus, as currently pled, Heritage Valley's Complaint sets forth facts which tend to establish that but for the 2003 Agreement, Nuance would not have provided Heritage Valley a secure private network connection, as the parties otherwise had no dealings with each other.

Accordingly, the negligence claim will be dismissed on the grounds of the gist of the action doctrine. As a consequence, absent a negligence claim, the demand for punitive damages and attorney's fees will be dismissed. Charles Shaid of Pennsylvania, Inc. v. George Hyman Const. Co., 947 F. Supp. 844, 849 (E.D. Pa. 2016), Merlino v. Delaware County, 728 A.2d 949, 951 (Pa. 1999)

B. Count II: Breach of implied contract

At Count II Plaintiff alleges breach of implied contract, in the alternative to Count I. The additional allegations as to this Count are as follows. Under the 2003 Agreement Dictaphone was provided to Heritage Valley through a trusted point-to-point virtual private network connection known as iChart. Compl. ¶ 69. Nuance subsequently acquired Dictaphone in 2006 and maintained the corporation as a wholly-owned subsidiary. Compl. ¶ 70. Heritage Valley continued to use the Dictaphone product having paid more than $3.1 million for its use of Dictaphone since the inception of the relationship. Compl. ¶ 71. In continuing to accept the benefits of this agreement and continuing to maintain this trusted connection Nuance impliedly contracted to take reasonable security measures to protect its computer network systems against cyber intrusion. Compl. ¶ 72. It is alleged that Nuance breached this implied contract by failing to adequately protect its computer network system against potential cyberattack and by failing to

protect its customers and the customers of its subsidiaries from becoming the collateral victim of a successful intrusion into one portion of Nuance's computer network systems. Compl. ¶ 73.

Defendant argues that this Count, too, should be dismissed, on the grounds that the Complaint does not allege any facts showing the existence of an implied contract with Nuance. Under Pennsylvania law, the elements of breach of an express contract are: "1) the existence of a contract, including its essential terms, (2) a breach of a duty imposed by the contract, and (3) resultant damages." CoreStates Bank, N.A. v. Cutillo, 723 A.2d 1053, 1058 (Pa. Super. 1999). The essential elements of breach of implied contract are the same as an express contract, except the contract is implied through the parties' conduct, rather than expressly written. Highland Sewer & Water Auth. v. Forest Hills Mun. Auth., 797 A.2d 385, 390 (Pa. Commw. 2002). Though intent can be gleaned from the parties' "ordinary course of dealing[s]," it is well-settled that "naked assertions devoid of further factual enhancement" fail to state an actionable claim. Liss & Marion P.C. v. Recordex Acquisition Corp., 603 Pa. 198, 983 A.2d 652, 659 (2009), Iqbal, 556 U.S. at 678.

As currently pled, Heritage Valley's Complaint sets forth facts which tend to establish that the parties continued to act as though the 2003 Agreement had not been terminated. In light of the terms of the 2003 Agreement and the allegations regarding the actions of the parties following expiration of the agreement and Nuance's purchase of Dictaphone, the Court concludes that any duty arises from the 2003 Agreement. Here, Plaintiff has not alleged sufficient facts to plausibly support an implied contract. Longenecker-Wells v. Benecard Serv. Inc., 658 Fed. Appx 659 (3d Cir. Aug. 25, 2016) (affirming motion to dismiss breach of implied contract as "naked assertions devoid of further factual enhancement failed to state actionable claim, noting there had been no contractual promise to safeguard information "especially from

third party hackers."); compare Enslin v. The Coca-Cola Co., 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015), aff'd sub nom. Enslin v. Coca-Cola Co., 739 F. App'x 91 (3d Cir. 2018) (denying motion to dismiss breach of implied contract because plaintiff alleged defendants through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard his personal identification information in exchange for his employment).

C. Count III: Unjust Enrichment

At Count III, Heritage Valley pleads an unjust enrichment claim against Nuance in the alternative to this implied contract claim at Count II, alleging that under these circumstances Nuance's continued retention of the benefits Nuance received under this relationship with Heritage Valley would be unjust. Compl. ¶¶ 75-79.

To state a claim for unjust enrichment under Pennsylvania law, a plaintiff must allege (1) that the plaintiff conferred a benefit on the defendant; (2) the defendant appreciated the benefit; and (3) the defendant accepted and retained the benefit under circumstances in which it would be inequitable to do so without paying for the benefit. *Karden Constr. Servs., Inc. v. D'Amico*, 219 A.3d 619, 628 (Pa. Super. 2019).

In Pennsylvania, "the doctrine of unjust enrichment is inapplicable when the relationship between parties is founded upon a written agreement or express contract." Wilson Area Sch. Dist. v. Skepton, 895 A.2d 1250, 1254 (Pa. 2006). Even where a contract would preclude recovery under unjust enrichment, a plaintiff may plead a claim for unjust enrichment in the alternative where "(i) the contract at issue covers only a part of the relationship between the parties, or [where] (ii) the existence of a contract is uncertain or its validity is disputed by the parties." Vantage Learning (USA), LLC v. Edgenuity, Inc., 246 F. Supp. 3d 1097, 1100 (E.D. Pa. 2017) (footnotes omitted) (citations omitted).

Unjust enrichment claim must be dismissed because under Pennsylvania law, unjust enrichment does not apply where there is a written contract that governs the relationship—"regardless of how 'harsh the provisions of such contracts may seem in the light of subsequent happenings.'" Wilson Area Sch. Dist. v. Skepton, 895 A.2d 1250, 1254 (Pa. 2006) (quoting Third Nat'l & Tr. Co. v. Lehigh Valley Coal Co., 44 A.2d 571, 574 (Pa. 1945)); see also Wingert v. T.W. Philips Gas & Oil Co., 157 A.2d 92, 94 (Pa. 1959) (holding that the unjust enrichment doctrine only applies in situations where a legal contract does not exist).

In its complaint Heritage Valley alleges as follows. Heritage Valley conferred a benefit on Nuance in the form of payments made to its wholly-owned subsidiaries, including Dictaphone Corporation. Compl. ¶ 76. Nuance appreciated these benefits which were commingled with its own revenues and the revenues of Nuance's other subsidiaries "for Nuance's own financial benefit." Compl. ¶ 77. Nuance failed to maintain adequate data security practices to protect Heritage Valley and other customers of its subsidiaries from becoming the indirect victim of a cyberattack, instead choosing to implement a business strategy focused on rapid international growth. Compl. ¶ 78. Under these circumstances, Heritage Valley alleges, it would be unjust for Nuance to retain the benefit of payments Heritage Valley has made to Nuance and its subsidiaries. Compl. ¶ 79.

Here, as discussed above, written contracts govern the disputed issues and frame the duty of care owed and obligations incurred. To the extent that Nuance should not have been paid as a result of the occurrence of the cyberattack, any such claim lies in contract.

D. Leave to Amend

Although a district court is not obligated to permit leave to amend before dismissing a complaint in a non-civil rights case, Wolfington v. Reconstructive Orthopaedic Assocs. II P.C.,

935 F.3d 187, 210 (3d Cir. 2019), courts generally grant leave to amend unless amendment of the complaint would be inequitable or futile. See, e.g., Bachtell v. Gen. Mills, Inc., 422 F. Supp. 3d 900, 915 (M.D. Pa. Oct. 1, 2019) (citing Phillips v. Allegheny Cty., 515 F.3d 224, 245 (3d Cir. 2008)). After a careful review of the claims set forth in the Complaint, we find that amendment would be futile.

IV. Conclusion

"Determining whether a complaint states a plausible claim for relief will ... be a context-specific task that requires the reviewing court to draw on its judicial experience and common sense." Iqbal, 556 U.S. at 679. For the foregoing reasons, the motion to dismiss is granted and the complaint is dismissed with prejudice.

An appropriate Order of Court will follow.

Dated: August 13, 2020

s/ Robert J. Colville
Robert J. Colville
United States District Judge

cc: All counsel of record via CM-ECF