IN THE SUPERIOR COURT OF THE STATE OF DELAWARE

TRAVELERS CASUALTY AND SURETY COMPANY OF AMERICA, Plaintiff, v. BLACKBAUD, INC., Defendant.	)	C.A. No. N22C-12-130 KMM
PHILADELPHIA INDEMNITY INSURANCE COMPANY, GREAT AMERICAN SPIRIT INSURANCE COMPANY, GREAT AMERICAN ALLIANCE INSURANCE COMPANY, ACADIA INSURANCE COMPANY, UNION INSURANCE COMPANY, Plaintiffs, v. BLACKBAUD, INC., Defendant.	)	C.A. No. N22C-12-141 KMM

Date Submitted: January 10, 2025
Date Decided: April 3, 2025

OPINION AND ORDER

Blackbaud, Inc.'s Motion to Dismiss Amended Complaints - ***GRANTED*.**

Wade A. Adams, Esquire, Law Offices of Wade A. Adams, III, Newark, Delaware; Marc S. Voses (*argued*), Clyde and Co., New York, New York; Kenneth T. Levine, Esquire, de Luca Levine LLC, East Norriton, Pennsylvania, *Attorneys for Plaintiff Travelers Casualty and Surety Company of America*

Lisa C. McLaughlin, Esquire, Todd L. Goodman, Esquire, Phillips, McLaughlin & Hall, P.A., Wilmington, Delaware; Kenneth T. Levine, Esquire (*argued*), de Luca Levine LLC, East Norriton, Pennsylvania, *Attorneys for Plaintiffs Philadelphia Indemnity Insurance Company, Great American Insurance Company, Great American Spirit Insurance Company, Great American Alliance Insurance Company, Acadia Insurance Company, and Union Insurance Company*

John P. DiTomo, Esquire, Elise K. Wolpert, Esquire, Morris, Nichols, Arsht & Tunnell LLP, Wilmington, Delaware; Sarah Fulton Hutchins, Esquire (*argued*), Parker Poe Adams & Bernstein LLP, Charlotte, North Carolina; Corri A. Hopkins, Esquire, Parker Poe Adams & Bernstein LLP, Raleigh, North Carolina, *Attorneys for Defendant Blackbaud, Inc.*

Miller, J.

I. *Introduction*

After their original breach of contract complaints were dismissed because they failed to identify any contractual terms or allege how they were breached, Travelers Casualty and Surety Company of America ("Travelers") and Philadelphia Indemnity Insurance Company, Great American Spirit Insurance Company, Great American Alliance Insurance Company, and Union Insurance Company (collectively, "Philadelphia Indemnity" and with Travelers, "Plaintiffs") filed amended complaints as subrogees of their respective insureds. Plaintiffs seek recovery of expenses they paid to their insureds for investigations, providing notifications to constituents, and credit monitoring, after Blackbaud, Inc. ("Blackbaud") suffered a ransomware attack. Blackbaud provided the insureds software solutions to manage their donors' personal identifying information, among other things.

The amended complaints are essentially identical. They identify Plaintiffs and the insureds and provide more factual detail about the contractual relationship between the insureds and Blackbaud. Each insured entered into a separate contract with Blackbaud, the terms of which are the same. Plaintiffs generally allege the types of data the insureds collectively stored in Blackbaud's software solutions, but do not provide facts specific to any insured. The amended complaints also allege that because of Blackbaud's contractual breaches, the insureds had to conduct their own investigations into the data breach and, at least some of them, had to comply

with privacy laws' notification requirements. The amended complaints do not identify any statute or regulation applying to the insureds individually.

Blackbaud moved to dismiss.

A subrogee stands in the shoes of the subrogor. Because the subrogee is entitled to no greater rights than the subrogor and the subrogee's claim is subject to the same defenses as the subrogor's, a plaintiff must allege the factual basis for the subrogor's underlying claim to properly allege a subrogation claim. While Delaware's pleading standard is minimal, for each element of the claim, a complaint must include specific allegations supported by facts. Pleading the insureds' claims in the aggregate, as Plaintiffs do, fails to provide the required factual support for any insured's claim and does not adequately allege a subrogation claim.

Even if pleading a multi-subrogor claim in the aggregate was sufficient, the amended complaints fail to adequately plead proximate cause because they fail to link the alleged damages to any contract term. The amended complaints allege that after the data breach, the insureds could not "rely" on Blackbaud's investigation and, as a result, they incurred expenses to conduct their own investigations of their obligations, if any, under applicable (but not identified) privacy laws. To plead proximate cause, Plaintiffs rely on a contractual term that required Blackbaud to mitigate negative consequences of a data breach. But when read in context, Plaintiffs' interpretation of the Blackbaud contract and thus, is not reasonable.

Plaintiffs' reliance on conclusory allegations of misrepresentations is also insufficient to adequately plead proximate cause.

As discussed below, the amended complaints fail to state a claim. Therefore, under Rule 12(b)(6), Blackbaud's motions to dismiss are **GRANTED**.

II. *Background*

A. *Plaintiffs and the Insureds*

Travelers issued insurance policies to 78 educational institutions and nonprofit entities[1] (the "Travelers Insureds"). Philadelphia Indemnity plaintiffs issued insurance policies to 25 educational institutions and nonprofit entities[2] (with the Travelers Insureds, the "Insureds"). The Insureds are spread across 35 states and the District of Columbia.

The policies provided coverage for certain cyber, criminal, and related incidents.[3] Under the policies, Plaintiffs have a right of subrogation for payments made to their Insureds.[4]

B. *The Contracts*

Blackbaud provides donor relationship management software and information technology to non-profit organizations, including charities, hospitals, and

[1] Travelers Amended Complaint (D.I. 34) ("T Am. Com."), ¶ 9.
[2] Philadelphia Indemnity Amended Complaint (D.I. 28) ("PI Am. Com."), ¶¶ 8-17.
[3] PI Am. Com., ¶ 18.
[4] PI Am. Com., ¶¶ 19, 21; T Am. Com., ¶ 12.

educational institutions. Each Insured entered into a separate "Solutions Agreement" with Blackbaud (the "Contracts").[5] Under the Contracts, Blackbaud provided subscriptions and services relating to its software products.

Blackbaud was contractually required to safeguard "Confidential Information" (defined to include: "(iii) donor, student, prospect and financial information")[6] using "commercially reasonable" cybersecurity procedures. Specifically, Section 6 of the Contracts provided:

> a. We[7] have implemented and will maintain administrative, physical, and technical safeguards designed to: (i) protect against anticipated threats or hazards to the security of Your Confidential Information, and (ii) protect against unauthorized access to or use of Confidential Information that could materially harm You. . . . We will at all times maintain commercially reasonable information security procedures and standards. . . .
>
> b. We have implemented commercially reasonable, written policies and procedures addressing potential Security Breaches and have a breach response plan in place.[8]

The Contracts required Blackbaud to notify the Insureds within 72 hours of discovering a "Security Breach," which is defined as "any unauthorized access, use, disclosure, modification, or destruction affecting the confidentiality of Your

[5] PI Am. Com., ¶¶ 27-29; T Am. Com., ¶¶ 18-20. A sample Contract is attached to each of the amended complaints. The Contracts incorporated Statements of Work and Order Forms. PI Am. Com., ¶ 28; T Am. Com., ¶ 19.
[6] PI Am. Com., Ex. 3, Section 5.a; T Am. Com., Ex. 3, Section 5.a.
[7] "We" and "Our" refer to Blackbaud. "You" and "Your" refer to the customer. "Us" refers to Blackbaud and the customer.
[8] PI Am. Com., Ex. 3, Section 6; T Am. Com., Ex. 3, Section 6.

Confidential Information."[9] In the event of a Security Breach, Blackbaud promised to "use commercially reasonable efforts to mitigate any negative consequences resulting directly from the Security Breach . . . ."[10]

Blackbaud represented and warranted that "it will comply with all applicable laws and regulations pertaining to this agreement,"[11] and that "[a]ll Services will be performed in a professional manner in accordance with industry standards."[12]

The Contracts contained a limitation of liability provision. Whether an action sounded in tort or contract, the Insured's recovery was limited to "the greater of (x) $25,000 or (y) the amount of fees paid or payable by You for the solution from which the claim arose during the six (6) months preceding the claim."[13] Further, the parties agreed that neither would "be liable for indirect, special, incidental, or consequential damages of any kind, even if a party has been advised of the possibility of such damages. You and Blackbaud agree to the allocation of risk set forth herein."[14]

[9] PI Am. Com., Ex. 3, Section 6.c; T Am. Com., Ex. 3, Section 6.c.
[10] PI Am. Com., Ex. 3, Section 6.d; T Am. Com., Ex. 3, Section 6.d.
[11] PI Am. Com., Ex. 3, Section 9.a.(iii); T Am. Com., Ex. 3, Section 9.a.(iii).
[12] PI Am. Com., Ex. 3, Section 9.b; T Am. Com., Ex. 3, Section 9.b.
[13] PI Am. Com., Ex. 3, Section 10. Original in all caps; T Am. Com., Ex. 3, Section 10. Original in all caps.
[14] PI Am. Com., Ex. 3, Section 10. Original in all caps; T Am. Com., Ex. 3, Section 10. Original in all caps.

The Contracts are governed by New York law,[15] and the parties agreed that the customer's "rights or obligations" under the Contracts "may not" be assigned without Blackbaud's written consent.[16]

C. *Information Hosted by the Insureds*

The amended complaints allege that the Insureds "possessed information concerning individuals," including personally identifiable information ("PII"), protected health information ("PHI"), and "proprietary and confidential information."[17] The amended complaints do not identify the type of information stored by any individual Insured.

D. *The Data Breach*

On February 7, 2020, an attacker gained access to "Blackbaud's self-hosted legacy product databases" and exfiltrated some data.[18] Blackbaud did not detect the intrusion until May 2020. The cybercriminal tried to lock Blackbaud out of the system, but its efforts were unsuccessful.[19] Blackbaud paid a ransom in exchange for the attacker deleting the exfiltrated data.[20]

---

[15] PI Am. Com., Ex. 3, Section 14; T Am. Com., Ex. 3, Section 14.
[16] PI Am. Com., Ex. 3, Section 17; T Am. Com., Ex. 3, Section 17.
[17] PI Am. Com., ¶¶ 32-34; T Am. Com., ¶¶ 23-25.
[18] PI Am. Com., ¶ 57; T Am. Com., ¶ 50.
[19] *Id.*
[20] PI Am. Com., ¶ 73; T Am. Com., ¶ 66.

Once detected, Blackbaud retained cybersecurity experts to investigate the attack.[21] "Blackbaud analyzed the exfiltrated file names to identify which products and customers were impacted, but Blackbaud did not analyze any of the contents of any of the exfiltrated files, and Blackbaud did not direct any of its third-party vendors to do so."[22] Through the investigation, Blackbaud learned that the cybercriminal accessed and exfiltrated over a million files "concerning over 13,000" Blackbaud customers, representing one-quarter of Blackbaud's customer base.[23]

E. *Blackbaud's Initial Customer Notification*

On July 14, 2020, Blackbaud's cybersecurity expert, Kudelski Security, issued its report on its investigation into the attack (the "Kudelski Report").[24] Two days later, Blackbaud disclosed the attack through a website posting and direct customer notification. The notification advised customers that "[t]he cybercriminals did not access credit card information, bank account information, or social security numbers. . . No action is required on your end because no personal information about your constituents was accessed."[25]

[21] PI Am. Com., ¶¶ 59-67; T Am. Com., ¶¶ 52-60.
[22] PI Am. Com., ¶ 76; T Am. Com., ¶ 69.
[23] PI Am. Com., ¶¶ 70-71, 78; T Am. Com., ¶¶ 63-64, 71.
[24] PI Am. Com., ¶ 60; T Am. Com., ¶ 53.
[25] PI Am. Com., ¶ 85; T Am. Com., ¶ 78. Plaintiffs allege that Blackbaud breached the Contracts by failing to give notice of the data breach within 72 hours. PI Am. Com., ¶ 184; T Am. Com., ¶ 179. But the amended complaints do not allege any damages that resulted from this alleged delay.

Blackbaud included a "Toolkit" in its customer notification. The Toolkit explained the scope of the data breach and outlined steps the customer should take to assess whether it had any further notification obligations. The Toolkit stated:

> **It is unlikely but possible, depending on jurisdiction, that our customers may have to make further notifications to constituents or other third parties.** We have built this step-by-step toolkit in the event you and your organization determine that you need to notify your constituents. The following toolkit should be used to ensure that you are taking the right steps in communicating efficiently and effectively with your constituents.
>
> We advise you to also consult with your organization's legal counsel to understand any notification requirements. We want to continue to be your partner through this incident. If you determine that you do need to notify your constituents, we have included templates in this toolkit to make it easier.
>
> This was a very sophisticated attack, and while we were able to defend against it for the most part, we realize this is still requiring that you invest time to review the situation, and that you may need to invest time to take follow-up actions.[26]

The Toolkit suggested that customers identify which laws govern in their jurisdictions.[27] The Toolkit advised customers that "[i]t's important to understand what kind of data your organization collects to determine your notification requirements."[28] The Toolkit also provided sample notification letters.

[26] PI Am. Com., Ex. 4, p. 3 (emphasis in original); T Am. Com., Ex. 4, p. 3 (emphasis in original).
[27] PI Am. Com., Ex. 4, p. 4; T Am. Com., Ex. 4, p. 4.
[28] PI Am. Com., Ex. 4, p. 4; T Am. Com., Ex. 4, p. 4.

F. *Blackbaud's Subsequent Disclosures*

A few days after the initial disclosure, Blackbaud learned that donor unencrypted "bank account information and social security numbers" "for a number of impacted customers" had in fact been accessed by the cybercriminal.[29]

Blackbaud, a public company, filed its Form 10-Q on August 4, 2020, disclosing the attack. The 10-Q did not include a disclosure about bank account information and social security numbers being accessed.[30] On September 29, 2020, Blackbaud filed an 8-K disclosing the full scope of the attack, including that bank account information and social security numbers had been exfiltrated.[31] Blackbaud sent supplemental notices to customers that Blackbaud believed had such donor information exfiltrated in the attack.[32]

G. *The Public Fallout from the Data Breach*

The data breach garnered a lot of public attention. Attorneys General from 49 states and the District of Columbia sued Blackbaud over its deficient data security safeguards and subsequent violations of state consumer protection laws, personal information protection laws, data breach notification laws, and HIPAA.[33] Blackbaud

[29] PI Am. Com., ¶¶ 87-88; T Am. Com., ¶¶ 80-81.
[30] PI Am. Com., ¶ 89; T Am. Com., ¶ 82.
[31] PI Am. Com., ¶ 91; T Am. Com., ¶ 84.
[32] PI Am. Com., ¶ 78, n.11, https://investor.blackbaud.com/node/22136/ixbrl-viewer.
[33] The federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). PI Am. Com., ¶¶ 94-99; T Am. Com., ¶¶ 87-92.

reached a settlement with the Attorneys General in 2023, paying $49.5 million.[34] In connection with the settlement, Delaware's Attorney General commented:

> This settlement resolves allegations of the attorneys general that Blackbaud violated state consumer protection laws, breach notification laws, and HIPAA by failing to implement reasonable data security and remediate known security gaps, which allowed unauthorized persons to gain access to Blackbaud's network, and then failing to provide its customers with timely, complete, or accurate information regarding the breach, as required by law. As a result of Blackbaud's actions, notification to the consumers whose personal information was exposed was significantly delayed or never occurred at all insofar as Blackbaud downplayed the incident and led its customers to believe that notification was not required.[35]

The Securities Exchange Commission ("SEC") also pursued charges against Blackbaud relating to the August 2020 10-Q.[36] Blackbaud resolved the claims by entering into a consent order. The order found that Blackbaud violated Sections 17(a)(1) and (2) of the Securities Act of 1933 and made factual findings, including that:

> By the end of July 2020, company personnel learned that the attacker had, in fact, accessed donor bank account information and social security numbers in an unencrypted form for a number of the impacted customers.
>
> ***
>
> Although the company's personnel were aware of the unauthorized access and exfiltration of donor bank account numbers and social security numbers by the end of July 2020, the personnel with this information about the broader scope of the impacted data did not

[34] *Id.*
[35] PI Am. Com., ¶ 94; T Am. Com., ¶ 87.
[36] PI Am. Com., ¶¶ 92-93; T Am. Com., ¶¶ 85-86.

> communicate this to Blackbaud's senior management responsible for disclosures, and the company did not have policies or procedures in place designed to ensure they do so.
>
> Moreover, in the company's discussion of its cybersecurity risks in the Form 10-Q, the company stated, "A compromise of our data security that results in ***customer or donor personal*** or payment card data being obtained by unauthorized persons ***could*** adversely affect our reputation with our customers and others, as well as our operations, results of operations, financial condition and liquidity and could result in litigation against us or the imposition of penalties." (Emphasis added). This statement omitted the material fact that such customer or donor personal data was exfiltrated by the attacker, which entailed that the risks of such an attack on the company's business were no longer hypothetical.[37]
>
> Blackbaud paid $3 million to resolve the charges.[38]

H. *Blackbaud's Cybersecurity Failures*

Plaintiffs allege that prior to the data breach, Blackbaud ignored warning signs that its cybersecurity measures exposed it to an attack. For example, Blackbaud maintained some unencrypted customer data on obsolete servers, which Blackbaud intended to migrate onto its new servers.[39] The older servers were not on a routine maintenance schedule, so security updates were not implemented.[40] Failure to run security patches on these older servers concerned Blackbaud employees.[41]

---

[37] Blackbaud's Opening Brief in Philadelphia Indemnity (D.I. 33), Ex. A (D.I. 37); Blackbaud's Opening Brief in Travelers (D.I. 39), Ex. A (D.I. 43) (emphasis in original).
[38] PI Am. Com., ¶ 92; T Am. Com., ¶ 85.
[39] PI Am. Com., ¶¶ 44-45; T Am. Com., ¶¶ 36-38.
[40] PI Am. Com., ¶¶ 45-46; T Am. Com., ¶¶ 38-39.
[41] PI Am. Com., ¶ 46; T Am. Com., ¶ 39.

Additionally, a former information security analyst warned Blackbaud about process vulnerabilities in its systems.[42] The analyst suggested that Blackbaud encrypt the obsolete servers, but "because the servers were so old, 'the exact nature of the data [on these servers] was unknown.'"[43] Plaintiffs allege that Blackbaud should have discontinued storing information on the obsolete servers given the potential for unauthorized access.

Blackbaud also failed to take heed of the analyst's warnings about remote desktop access vulnerabilities.[44] Blackbaud knew the risk was so high that employees would "simply shut down certain machines at times."[45]

Failures in Blackbaud's systems were further revealed in the Kudelski Report. It identified steps that Blackbaud could have taken to prevent an attack, including requiring customers to use multifactor authentication. Because Blackbaud had not implemented this security measure, the cybercriminal was able to use a customer's password to access the system and then "freely move across multiple Blackbaud-hosted environments by leveraging existing vulnerabilities . . . ."[46]

Blackbaud also failed to require customers to encrypt social security numbers and bank account information stored in certain fields on the system.[47]

---

[42] PI Am. Com., ¶¶ 47-48; T Am. Com., ¶¶ 40-41.
[43] PI Am. Com., ¶ 49; T Am. Com., ¶ 42.
[44] PI Am. Com., ¶ 48; T Am. Com., ¶ 41.
[45] *Id*.
[46] PI Am. Com., ¶ 63; T Am. Com., ¶ 56.
[47] PI Am. Com., ¶¶ 114-15; T Am. Com., ¶¶ 107-08.

Finally, Blackbaud retained some current and former customers' data for years longer than needed, unnecessarily exposing this data to a cyber breach.[48]

I. *Insureds' Response to Data Breach*

Plaintiffs allege that Blackbaud's initial notice of the data breach led the Insureds to believe that they had no further notification obligations.[49] So, "each Insured had to investigate the detailed identity and other information as to involved persons and their data (residency of individuals; nature of private data; nature of how and where such data was input into Blackbaud's system or software; and relevant laws that may need compliance)."[50] Blackbaud's changing notification about the scope of the data breach gave Insureds "no comfort that Blackbaud was upholding its contractual obligations or providing them with sufficient information to be able to reasonably rely on Blackbaud's investigation" and because the Insureds were subject to various privacy laws, they "were forced to undertake independent investigations" to determine their obligations and provide notification, if required.[51]

The Insureds incurred expenses to investigate and comply with their obligations under applicable laws.[52] Collectively, the expenses included: (i)

[48] PI Am. Com., ¶¶ 116-17; T Am. Com., ¶¶ 109-10.
[49] PI Am. Com., ¶ 100; T Am. Com., ¶ 93.
[50] PI Am. Com., ¶ 101; T Am. Com., ¶ 94.
[51] PI Am. Com., ¶¶ 103-04, 125; T Am. Com., ¶¶ 96-97, 118.
[52] There are no allegations that any of the Insureds' own data was compromised.

retaining computer forensics firms to identify the type of information the Insured stored in the Blackbaud software, the identity of the Insured's donors, and the date of the breach; (ii) outside counsel fees incurred in determining which state/federal data breach laws applied, whether notifications were required and if so, drafting the notification, and generally providing legal advice; (iii) retaining printing and mailing firms to send notifications; (iv) communicating with Blackbaud regarding the scope of the breach and remedial steps; and (v) credit monitoring "required under various state laws and expected by federal regulators" (the "Expenses").[53] These Expenses were paid by the applicable Plaintiff, except to the extent that the policy contained a deductible.

Travelers' amended complaint includes a list of its Insureds, identifying the name and principal location of the Insured, the applicable deductible paid by the Insured, and the amount Travelers paid to each Insured.[54] Travelers seeks recovery of $1,558,086.39 that it paid to its Insureds and $550,000 in deductibles incurred by certain of its Insureds.[55]

[53] PI Am. Com., ¶¶ 140-41, 161; T Am. Com., ¶¶ 134-35, 156. Travelers' Answering Brief (D.I. 44) ("T AB") at p. 7.
[54] T Am. Com., Ex. 2.
[55] T Am. Com., ¶¶ 135-37.

Philadelphia Indemnity's amended complaint identifies its Insureds and states a total amount paid on their behalf in the aggregate, which is "in excess of $600,000."[56] It does not provide a breakdown of these amounts by each Insured.

J. *Blackbaud's Contractual Breaches*

Plaintiffs allege that Blackbaud breached the Contracts in several ways. First, Blackbaud failed to maintain commercially reasonable cybersecurity as promised and represented in the Contracts.[57] Second, Blackbaud failed to provide timely notice and when it did provide notice, Blackbaud "made false representations concerning the scope" of the breach.[58]

---

[56] PI Am. Com., ¶¶ 140-41.

[57] PI Am. Com., ¶¶ 169-73, 177-82; T Am. Com., ¶¶ 164-68, 172-77. In addition to the alleged security failures described above, Plaintiffs incorporate security failures alleged by the Federal Trade Commission. PI Am. Com., ¶ 118; T Am. Com., ¶ 111. Plaintiffs also incorporate allegations made by the Attorneys General (PI Am. Com., ¶ 95; T Am. Com., ¶ 88) but do not identify any of those allegations.

[58] PI Am. Com., ¶¶ 121, 183-88; T Am. Com., ¶¶ 113, 178-83. Plaintiffs allege that the July disclosure was materially misleading and contained misrepresentations. This accusation is based on Blackbaud later revealing that some bank account and social security information was accessed by the attacker. But the amended complaints contain no factual support for the contention that Blackbaud knew that its description of the scope of the attack was inaccurate at the time of the initial disclosure.

Plaintiffs seem to rely on the SEC settlement to support the misleading disclosure allegation, but the SEC Consent Order does not suggest that the August 2020 10-Q was intentionally misleading. Rather, Blackbaud was lacking an internal process to communicate information regarding the scope of the breach to upper management, who were responsible for issuing the 10-Q.

To the extent the amended complaints attempt to assert that the July disclosure was intentionally misleading, this allegation has no factual support. The court does not accept conclusory allegations as true on a motion to dismiss. *Cent. Mortg. Co. v. Morgan Stanley Mortg. Cap. Holdings LLC*, 27 A.3d 531, 535, 536-37, n.13 (Del. 2011).

Third, Blackbaud "passed the buck" on its obligations after the data breach. Plaintiffs assert that Blackbaud was contractually required to investigate for each Insured: the scope of the data stored by the Insured; the privacy laws which applied to the Insured; and whether donor notification was required, and where notification was required by law, Blackbaud was to draft and send such notifications. Plaintiffs point to the Toolkit as Blackbaud "admit[ting]" that remediation expenses, such as the Expenses, were a necessary result of the data breach.[59] For example, the Toolkit "instructed" Insureds to consult with legal counsel, determine what laws applied to them, "partner with Blackbaud" through the data breach, and to use the provided templates. The Toolkit "acknowledged" that it was important for the customers to understand the type of data they stored and that laws of the jurisdiction where the donors reside may be implicated, in addition to the jurisdiction where the Insured was located.[60] Blackbaud is alleged to have breached these obligations by failing to provide "crucial information" and not performing these services.

Fourth, while Blackbaud represented that it would comply with all applicable laws and regulations, including data breach notification laws, and would perform services in a professional manner, it did not do so.[61]

[59] PI Am. Com., ¶¶ 145-46; T Am. Com., ¶¶ 140-41.
[60] PI Am. Com., ¶¶ 149-55; T Am. Com., ¶¶ 144-50.
[61] PI Am. Com., ¶¶ 174-75; T Am. Com., ¶¶ 169-70.

III. *The Parties' Contentions*

Blackbaud asserts three grounds for dismissal. First, the amended complaints improperly lump the Insureds' claims, providing no Insured-specific factual allegations. Second, the amended complaints lack any factual support to show that the Expenses were proximately caused by any alleged contractual breach. Third, the Expenses are consequential damages, which are expressly barred by the Contracts. Fourth, Travelers lacks standing to recover the deductibles because the Contracts prohibit assignment without Blackbaud's consent.

Plaintiffs respond that it is permissible to aggregate the Insureds' claims, pointing out that no Delaware case requires the level of detail urged by Blackbaud. Further, damages may be generally alleged, and so the amended complaints sufficiently allege proximate cause.

Plaintiffs argue that the Expenses are direct damages and thus, the contractual damages-limitation provision does not apply. Additionally, whether damages are direct or consequential is a fact question, which cannot be decided at this stage of the litigation. And even if the Expenses are consequential damages, the limitations clause is unenforceable under New York law.

Finally, Travelers asserts that Blackbaud's consent is not required for the Insureds to validly assign their claims to it, and therefore, Travelers has standing to assert the deductible claim.

IV. *Standard of Review*

Because the Contracts provide that they are governed by New York law, the Court will apply New York substantive law. Delaware procedural law applies.[62]

Under Superior Court Civil Rule 12(b)(6), the court accepts as true all well pleaded factual allegations and draws all reasonable inferences in favor of the non-moving party. Dismissal will be denied if there is a reasonably conceivable set of circumstances of recovery on the claim.[63]

Delaware's pleading standard is "minimal," but the liberal construction afforded to a claimant does not "extend to 'conclusory allegations that lack specific supporting factual allegations.'"[64] Accordingly, the court should dismiss a complaint if the plaintiff fails to make "specific allegations supporting each element of a claim or if no reasonable interpretation of the alleged facts reveals a remediable injury."[65]

---

[62] *US Dominion, Inc. v. Fox News Network, LLC*, 2021 WL 5984265, at *18 (Del. Super. Dec. 16, 2021) (as a general matter, the law of the forum governs procedural matters).
[63] *Cent. Mortg. Co.*, 27 A.3d at 536-37, n.13.
[64] *Id.; Surf's Up Legacy Partners, LLC v. Virgin Fest, LLC*, 2021 WL 117036, at *6 (Del. Super. Jan. 13, 2021) (quoting *Ramunno v. Cawley*, 705 A.2d 1029, 1034 (Del. 1998)).
[65] *Axogen Corp. v. Integra LifeSciences Corp.*, 2021 WL 5903306, at *2 (Del. Super. Dec. 13, 2021) (citing *Surf's Up*, 2021 WL 117036, at *6).

V. *Discussion*

A. *Breach of Contract Elements*

To state a claim for breach of contract, a plaintiff must allege "(1) the existence of a contract; (2) that the contract was breached; and (3) damages suffered as a result of the breach."[66] Each element must be supported by specific factual allegations; conclusory statements are insufficient.[67] Generally referring to a contract will not sustain a claim. "A party must identify the particular contractual terms that were breached."[68]

B. *Do the Amended Complaints Adequately Plead Subrogation Claims?*

Relying on three New York cases, Blackbaud argues that Plaintiffs are required to separately plead each individual Insured's claim. Therefore, the amended complaints, which lump the Insureds' claims together, are insufficient.

Plaintiffs assert that Blackbaud is improperly applying New York procedural law by relying on these cases. Plaintiffs distinguish these cases and, relying on a different New York case, argue that they have sufficiently alleged the claims because

---

[66] *Patriarch Partners, LLC v. Zohar CDO 2003-1, LLC*, 2017 WL 2643972, at *1, n.3, 165 A.3d 288 (TABLE) (Del. 2017) (applying New York law).

[67] *Festival Fun Parks, LLC v. MS Leisure Co.*, 2023 WL 8714994, at *4 (Del. Super. Dec. 18, 2023).

[68] *Marydale Preservation Associates, LLC v. Leon N. Weiner & Associates, Inc.*, 2022 WL 4446275, at *17 (Del. Super. Sept. 23, 2022); *Clifden Futures, LLC v. Man Fin., Inc.*, 858 N.Y.S.2d 580, 583-84 (N.Y. Sup. 2008) ("The pleadings must be sufficiently particular to give the court and [the] parties notice of the transaction, occurrences, or series of transactions or occurrences, intended to be prove as well as the material elements of each cause of action or defense." (quoting *Atkins v. Mobil Oil Corp.*, 614 N.Y.S.2d 36 (2d Dep't 1994) (citation omitted)).

the group of Insureds is clearly defined and known to Blackbaud, with each having the same contractual relationship with Blackbaud which was breached by the same acts or omissions, and each suffered expenses in the same way. Plaintiffs assert that details of each Insured's claim can be developed through discovery.

Blackbaud counters that it is not attempting to apply New York procedural law, but no Delaware case has addressed the pleading requirements for a multi-subrogor claim.[69]

Subrogation is not a separate cause of action; it is purely derivative.[70] It is "'the substitution of one person in the place of another with reference to a lawful claim or right.'"[71] Subrogation allows one person "to stand in the shoes of another and assert that person's rights against a third party."[72] The subrogee has no greater rights than its subrogor.[73] Accordingly, a subrogee must allege the factual basis for the subrogor's claim against the third party.

---

[69] No party cited Delaware cases and the Court's research revealed no case addressing this issue. Thus, it appears to be a matter of first impression.
[70] 73 Am.Jur.2d *Subrogation* §§ 1, 75.
[71] *Jefferies v. Kent Cnty. Vocational Sch. Dist. Bd.*, 743 A.2d 675, 678 (Del. Super. 1999) (quoting 73 Am.Jur.2d *Subrogation* § 1).
[72] 73 Am.Jur.2d *Subrogation* § 1; *Rodriguez v. Great Am. Ins. Co.*, 2022 WL 591762, at *7 (Del. Super. Feb. 23, 2022) ("subrogation allows a third-party to replace one of the parties to a contract and then assume the right of that contracting party to sue the counterparty."); *Servidori v. Mahoney*, 515 N.Y.S.2d 328, 329 (N. Y. App. 1987) (" A subrogee acquires all rights, defenses and remedies of the subrogor and is subject to any claims or defenses which may be raised against the subrogor; thus, the rights of a subrogee must be determined with respect to the rights of the subrogor.") (citation omitted).
[73] *Rodriguez*, 2022 WL 591762, at *9.

Rule 8 requires a "short and plain statement of the claim showing that the pleader is entitled to relief."[74] Only well-pleaded allegations, which are "specific allegations of fact and conclusions supported by specific allegations of fact," will be accepted as true for purpose of a Rule 12(b)(6) motion.[75]

A subrogation claimant must assert well-pleaded allegations of fact to show that the *subrogor* has a valid claim against the defendant, and in a multi-subrogor action, a plaintiff must separately plead facts for each. Here, the amended complaints run afoul of the pleading requirements because Plaintiffs do not allege Insured-specific facts. The amended complaints allege that the Insureds investigated what data they stored, but do not identify the data stored by each. There are no allegations that any Insured stored bank account information or social security numbers—the very information that was allegedly compromised—or that any Insured received the supplemental Blackbaud notice.[76] The amended complaints merely contain blanket allegations that various types of data *may* have been stored by various Insureds.[77]

---

[74] Super. Ct. Civ. R. 8(a).
[75] *White v. Panic*, 783 A.2d 543, 549, n.12 (Del. 2001); *Spencer v. Spencer*, 2012 WL 1495324, at *2 (Del. Super. Apr. 20, 2012) (same).
[76] Blackbaud acknowledged that the attacker accessed "unencrypted donor bank account information and social security numbers for certain of the impacted customers . . . ." PI Am. Com., ¶ 90; T Am. Com., ¶ 83.
[77] Of course, the type of data stored impacts whether an Insured had any reporting or notification obligations under privacy laws.

Additionally, the amended complaints do not allege what privacy law requirements any Insured allegedly had to satisfy. The amended complaints simply cite to a third-party vendor's website containing a survey of the 50 states' privacy laws. The amended complaints do not allege which, if any, of the listed laws applied to each Insured. Plaintiffs admit that no Insured relied on this webpage or even viewed it.

Plaintiffs argue that they do not need to identify the specific privacy statutes because at this stage of the proceedings, the Court is required to accept their allegations as true. The requirement that the Court accept the non-movant's allegations as true, however, only applies to well-pleaded allegations; *i.e.*, allegations supported by facts.[78] Conclusory allegations, or allegations that are so vague that they do not provide fair notice of the claims being asserted, will not be accepted as true.

Finally, the amended complaints do not include Insured-specific factual allegations of the type(s) of Expenses allegedly incurred.

Without providing the factual information for each Insured's claim, Blackbaud, and the Court, cannot assess whether the subrogor-Insureds have a valid claim against Blackbaud.

[78] *Clinton v. Enter. Rent-A-Car Co.*, 977 A.2d 892, 895 (Del. 2009) (the court will not "accept conclusory allegations unsupported by specific facts or to draw unreasonable inferences in favor of the non-moving party.").

The Court's conclusion is supported by the cases relied upon by Blackbaud.[79] In these cases, healthcare providers and insurers asserted claims against tobacco companies seeking to recover healthcare costs paid for patients or plan subscribers, whose medical conditions were caused or exacerbated by tobacco use. The plaintiffs did not identify the subrogors in the complaints. The courts ruled that "[a]t the very least," the plaintiffs were required to identify the subrogors "*and those subrogors' claims so that defendants would have the opportunity to assert defenses against those claims*."[80]

Plaintiffs attempt to distinguish these cases by arguing that, unlike them, the amended complaints identify the subrogors by name, identify the types of expenses incurred by the Insureds (and for Travelers, the amount for each), and the basis for Blackbaud's liability.[81] But, as explained above, Plaintiffs did not provide a factual basis for *each* Insured's claim.

---

[79] *Blue Cross & Blue Shield of New Jersey, Inc. v. Philip Morris USA Inc.*, 344 F.3d 211 (2d Cir. 2003); *A.O. Fox Mem'l Hosp. v. Am. Tobacco Co., Inc.*, 754 N.Y.S.2d 368 (N.Y. App. 2003); *E. States Health & Welfare Fund v. Philip Morris, Inc.*, 729 N.Y.S.2d 240 (N.Y. Sup. 2000).

[80] *Blue Cross*, 344 F.3d at 218 (emphasis added). *See also E. States Health*, 729 N.Y.S.2d at 252 ("Without ascertaining what the specific injuries are for each person, and without the ability to demonstrate what other factors may have caused the injuries, Defendants cannot fairly defend the [] claims."); *A.O. Fox Mem'l Hosp.*, 754 N.Y.S.2d at 414 ("plaintiffs failed to identify the individual patients and their particular injuries and specify facts which, if proven, would establish liability.").

[81] T AB at p. 12; Philadelphia Indemnity Answering Brief (D.I. 39) ("PI AB") at p. 12.

The case Plaintiffs rely on, *Lawyers' Fund,*[82] is distinguishable. It involved a subrogation claim that arose out of an attorney's misappropriation of clients' money from the attorney's escrow account. After the Lawyers Fund reimbursed the clients, it asserted claims against the bank where the escrow account was held. The original complaint was dismissed for failing to provide sufficient facts supporting each clients-subrogors' claims. The amended complaint included the identity of the clients and pled "separate causes of action which particularized each claimant's losses and the specific reasons why the misappropriated funds had been deposited into the escrow account."[83] The *Lawyers' Fund* court ruled that the amended complaint adequately pled the subrogation claim.

The *Lawyers Fund* court noted in its ruling that the group of subrogors was "small, clearly defined and readily identifiable" and not unknown to the bank, and that their losses arose from the same attorney relationship and the bank's same acts and omissions.[84] Plaintiffs make the same argument here: the amended complaints adequately plead subrogation claims because the Insureds are known to Blackbaud, all suffered a loss resulting from the data breach, and the amended complaints

[82] *Lawyers' Fund for Client Protection of the State of N.Y. v. JP Morgan Chase Bank, N.A.* 915 N.Y.S.2d 741 (N.Y. App. 2011).
[83] 915 N.Y.S. at 742.
[84] *Id*. at 742-43.

describe the types of expenses incurred by the Insureds, and as for Travelers, the amount each incurred.

The difference here is that Plaintiffs do not separately plead the claim of each Insured, supported by Insured-particular facts. Rather, the amended complaints list a series of actions taken and expenses incurred by the collective, unrelated group of Insureds.

At the outset of litigation, a defendant is entitled to fair notice of the claims asserted against it so that it may develop its defenses.[85] Because Plaintiffs aggregate the Insureds' claims, Blackbaud does not have the opportunity to assert defenses to the independent claims. As pled, the amended complaints do not allege sufficient factual support that any Insured has a cause of action against Blackbaud and therefore, do not assert a valid subrogation claim.

C. *Do the Amended Complaints Adequately Plead Breach of Contract?*

Blackbaud argues that the amended complaints fail to adequately plead that the Expenses were proximately caused by the alleged breach of contract. The amended complaints contain no facts that any Insured's data was (1) in the Blackbaud solutions impacted by the data breach, or (2) the type that would require further action by an Insured. Blackbaud further argues that Plaintiffs point to no

[85] *See In re Benzene Litig.*, 2007 WL 625054, at *6 (Del. Super. Feb. 26, 2007).

contractual provision that allows the Insureds to recover Expenses due to the Insureds' inability to "rely on" Blackbaud's investigation.

Plaintiffs respond that it does not matter whether an Insureds' data was affected by the data breach because the Insureds could not rely on Blackbaud's investigation. Thus, each was forced to conduct its own investigation, as the Toolkit suggested. Some of the Insureds allegedly were required to take further steps of providing constituent notification and responding to regulators. Plaintiffs argue that the identity of these Insureds can be developed through discovery.[86]

1. *Plaintiffs' Interpretation of the Contract is Unreasonable*.

While damages may be pled generally, a factual basis connecting the alleged injury to the breach is required; that is, a plaintiff must provide a factual basis for proximate cause.[87] To link the Expenses to the Contracts, Plaintiffs rely on Blackbaud's contractual promise to mitigate the impact of a data breach. As Plaintiffs interpret the Contracts, Blackbaud's promise to "mitigate any negative consequences resulting directly from the Security Breach" required it to determine what type of data each Insured stored in Blackbaud's software, research each

[86] Plaintiffs argue that because they sent Blackbaud information on each Insured, Blackbaud knows the scope and extent of the Insureds' damages. T AB at p. 15, n.6 (D.I. 44); PI AB at p. 15, n.6 (D.I. 39). The Court is constrained to the allegations in the complaint and the documents incorporated therein. So, what Plaintiffs may have provided Blackbaud cannot be considered on a motion to dismiss.

[87] *Wellgistics, LLC v. Welgo, Inc.*, 2024 WL 113967, at *5 (Del. Super. Jan. 9, 2024) (citing *Phage Diagnostics, Inc. v. Corvium, Inc.*, 2020 WL 1816192, at *9 (Del. Super. Mar. 9, 2020)).

Insured's obligations under various privacy laws that may apply to it, and, where required, draft and send notifications. The problem with this interpretation is that it proves too much.

The Contracts define "Security Breach" as "any unauthorized access, use, disclosure, modification, or destruction affecting the confidentiality of Your Confidential Information."[88] Blackbaud agreed to maintain "commercially reasonable information security procedures and standards."[89] If a Security Breach occurred due to Blackbaud's failure to maintain this level of security, it would breach the Contract.[90]

No cybersecurity system is full-proof.[91] Blackbaud's agreement to "mitigate any negative consequences resulting directly from the Security Breach" is not limited to a breach resulting from a failure to maintain commercially reasonable security measures. The duty to mitigate applies to *any* data breach, no matter the cause. Under Plaintiffs' interpretation, Blackbaud contractually agreed that for every data breach – an "at-fault" breach or a "no-fault" breach – Blackbaud would undertake an investigation for *every customer* and provide notification where

[88] PI Am. Com., Ex. 3, Section 6.c; T Am. Com., Ex. 3, Section 6.c.
[89] PI Am. Com., Ex. 3, Section 6.a; T Am. Com., Ex 3, Section 6.a.
[90] Plaintiffs also argue that Blackbaud breached the Contracts by failing to comply with applicable laws relating to the Contracts (*see* PI Am. Com., ¶ 190; T Am. Com., ¶ 185), but they do not identify any law that Blackbaud allegedly violated that caused the Insureds to incur the Expenses.
[91] *See Travelers Cas. & Sur. Co. of Am. v. Blackbaud, Inc.*, 2024 WL 1298762, at *2 (Del. Super. Mar. 27, 2024) (noting that in 2022, 83% of organizations experienced more than one data breach).

required.

Plaintiffs' interpretation of the Contracts is not reasonable.[92] Blackbaud agreed with each Insured to a risk allocation in the event of a breach of contract or a tort claim, including a data breach. This risk allocation capped the amount of damages an Insured could recover from Blackbaud[93] and limited the types of damages recoverable. While the parties spar over whether the Expenses are consequential damages and whether the waiver of such damages is enforceable under New York public policy, the inclusion of the limitation clause demonstrates the parties' intent to allocate the risk of loss in the event that Blackbaud breaches the Contract or commits a tort.[94]

Yet, as Plaintiffs would have it, a no-fault data breach would require Blackbaud to perform the same investigation and provide the same notifications as a data breach that resulted from a breach of contract or a tort. It is not reasonable to construe the Contracts to essentially impose strict liability on Blackbaud for every data breach when the parties expressly agreed to a risk allocation scheme. Thus, the

---

[92] Interpretation of an unambiguous contract is a legal question for the Court to decide. *See NCCMI, Inc. v. Bersin Properties, LLC*, 208 N.Y.S.3d 27, 33 (N.Y. App. 2024) ("a 'contract should not be interpreted to produce a result that is absurd, commercially unreasonable or contrary to the reasonable expectations of the parties.'" (citation omitted)); *see also Sunline Com. Carriers, Inc. v. CITGO Petroleum Corp.*, 206 A.3d 836, 847 (Del. 2019).

[93] The Contracts limited the Insureds' damages to the greater of $25,000 or the amount the customer paid in the six months preceding the incident.

[94] *Matter of Part 60 Put-Back Litig.*, 141 N.Y.S.3d 410, 416 (N.Y. App. 2020) (New York courts enforce contractual limitations on damages "because those provisions represent the parties' agreement on the allocation of the risk of economic loss in certain eventualities.").

mitigation clause does not provide a causal link between the Contracts and the Expenses, as Plaintiffs assert. Because the Expenses are untethered to any contractual term, Plaintiffs failed to adequately plead proximate cause.

2. *Aspen is Distinguishable.*

Plaintiffs rely on another case that arose out of the same Blackbaud data breach—*Aspen American Ins. Co. v. Blackbaud, Inc.*[95]—to argue that they have adequately pled proximate cause. In this case, Trinity Health Corporation ("Trinity"), a multi-facility healthcare system, maintained sensitive donor and patient PHI and PII. Trinity entered into two contracts with Blackbaud to manage this data: a Master Application Services Provider Agreement and a Business Associate Agreement. Under these contracts, Blackbaud agreed that within 10 days of a data breach, Blackbaud would provide Trinity a report identifying each patient whose PHI had been accessed and to "cooperate to the extent practical with [Trinity] in mitigating . . . any harmful effect that is known to [the] Business Associate to a use or disclosure of PHI."[96]

Trinity's PHI and PII were stored on the obsolete Blackbaud servers. After the data breach, Blackbaud provided Trinity with a report, but it did not include the detailed identification information that Trinity needed in order to notify patients

[95] 2023 WL 3737050 (N.D. Ind. May 31, 2023).
[96] 2023 WL 3737050, at *2.

affected by the breach. Blackbaud "declined to participate" any further in the process.[97]

Due to Blackbaud's failure to provide the detailed information and cooperate as contractually required, Trinity investigated and determined that approximately 3.2 million of its patients had their PHI compromised, and the information impacted was unencrypted.[98] Trinity determined that under HIPAA and Guidance Documents from the Department of Health and Human Services, it was required to send notification to these patients.[99] Trinity and its insurer, Aspen American Insurance Company, filed an amended complaint against Blackbaud seeking recovery for the investigation, the costs of notifications, and expenses associated with mitigation provided to the patients.[100]

The *Aspen* court found that the amended complaint adequately alleged causation because the plaintiffs provided detailed factual allegations that Trinity: (1) was required to conduct its own investigation because Blackbaud failed to fulfill its contractual obligation to provide the report and cooperate; (2) identified specific statutes and regulations that led it to conclude that it was required to send notifications; and (3) identified specific regulations and rules that Trinity considered

[97] *Id.*
[98] *Id.*
[99] *Id.*
[100] *Id.*

in determining that it was required to provide patients with credit monitoring.[101] Plaintiffs argue that the same reasoning applies here.

But *Aspen* is distinguishable. First, the contracts are different. Blackbaud was required to provide Trinity a report that identified each patient whose PHI or PII was compromised. The Contracts impose no such requirement on Blackbaud. Second, the plaintiffs in *Aspen* identified the information stored by Trinity and where it was stored on Blackbaud's system, what information was impacted, and the statutes and regulations with which it believed it was required to comply. The amended complaints provide no such factual details. As such, *Aspen* provides no support for Plaintiffs.

3. *Plaintiffs' Conclusory Proximate Cause Allegation are Insufficient.*

Finally, Plaintiffs attempt to connect the Expenses to the Contracts by asserting that Blackbaud's misrepresentations of the scope of the data breach caused the Insureds to conduct their own investigations, because they could not "reasonably rely on Blackbaud's investigation into" the data breach.[102] Plaintiffs also argue that the amended complaints do allege the Expenses were proximately caused by Blackbaud's breaches, citing to Philadelphia Indemnity's paragraph 191 and Travelers' paragraph 186.[103]

---

[101] *Id.*, at *11-13.
[102] PI Am. Com., ¶¶ 103, 125, 139; T Am. Com., ¶¶ 96, 118, 133.
[103] PI AB at p. 27; T AB at p. 28.

Plaintiffs' argument fails for two reasons. First, there is no "reasonable reliance" term in the Contracts. Plaintiffs do not point to any contractual provision that grants an Insured a right to declare Blackbaud's investigation unreliable, nor do the amended complaints allege that any Insured actually made such a determination.

The amended complaints also do not allege when any Insured conducted its investigation.[104] If the investigations started after the July notice, when it was unknown that banking information and social security numbers were compromised, then the investigations could not have been proximately caused by Blackbaud's allegedly unreliable investigation. No one knew at the time that the initial disclosure was incorrect. Additionally, there are no allegations that any Insured received the supplemental Blackbaud notice or relied on the September 8-K that reported on the full scope of the breach. So even if there was a "reasonable reliance" term in the Contracts, there is no factual support that the Insureds' investigations were proximately caused by Blackbaud's initial incorrect disclosure.[105]

[104] The amended complaints actually seem to suggest that the investigations started after the July notice. Plaintiffs allege that after the Insureds received notification of the data breach, each Insured had to investigate. PI Am. Com., ¶ 101; T Am. Com., ¶ 94. The amended complaints only allege that the Insureds received the July notice.

[105] Plaintiffs acknowledged at oral argument that had a Blackbaud customer, as an entity storing sensitive donor information, researched the laws that would apply to it in the event of a data breach *before* the 2020 data breach occurred, that customer would not be able to seek recovery of the cost of that research from Blackbaud. That an Insured undertook this research after the data breach is, alone, insufficient to plead proximate cause. *Travelers Cas. and Surety Co. of Am. v. Blackbaud, Inc.*, 2024 WL 1298762, at *11 (Del. Super. Mar. 27, 20204) ("The Insureds may have undertaken this work after receiving a breach notice, but the timing alone is insufficient.").

Second, the amended complaints' allegations of proximate cause are conclusory. Plaintiffs allege that:

> [a]s a direct and proximate result of Blackbaud's breaches, as noted above, the Insureds were required to comply with numerous state and federal statutes and regulations, which compelled them to retain legal experts to assess and comply with such laws following exposure or possible exposure of private data; to retain computer experts to investigate the breadth of the data breach and the private data involved; and to retain firms (or to incur costs themselves) to comply with data breach notification laws.[106]

Plaintiffs provide no factual support identifying the "numerous state and federal statutes."[107] Such conclusory allegations are insufficient to adequately plead proximate cause.

VI. *Conclusion*

The amended complaints fail to properly allege subrogation claims because they fail to provide any factual support for each Insured's claim. The amended complaints also fail to assert well-pleaded allegations of proximate cause. Therefore, the motions to dismiss are **GRANTED**. Because this was Plaintiffs'

---

[106] PI Am. Com., ¶ 191; T Am. Com., ¶ 186.

[107] Plaintiffs argue that the amended complaints citing to the website, which then incorporates each state's data breach notification laws, is sufficient under Delaware's pleading standard, citing *Alvarez v. Cooper Tire & Rubber Co.*, 2013 WL 226970, at *3, n.57 (Del. Super. Jan. 18, 2013). In *Alvarez*, the complaint asserted that the defendant violated the "Consumer Protection Act." Because there is no such act in Ohio (the law that applied), defendant moved for summary judgment. Noting that a simple internet search revealed that the act was titled the "Ohio Consumer Sales Practices Act," the court denied the motion. But the court required plaintiffs to file an amended complaint "specifically identifying all statutes they allege Defendant violated." Thus, *Alvarez* does not stand for the proposition that citing to a website that compiles hundreds of laws is sufficient to put a defendant on notice of the claims against it.

second attempt to adequately plead their claims, the amended complaints are ***dismissed with prejudice***.

Because of the Court's rulings on subrogation and breach of contract, it does not reach the remainder of the parties' arguments.

IT IS SO ORDERED.

/s/Kathleen M. Miller
Kathleen M. Miller, Judge