EFiled: Jun 24 2025 12:30PM EDT
Filing ID 76519947
Case Number 198,2025

IN THE SUPREME COURT OF THE STATE OF DELAWARE

PHILADELPHIA INDEMNITY INSURANCE COMPANY, ACADIA INSURANCE COMPANY, and UNION INSURANCE COMPANY Plaintiffs-Below/Appellants,	:	C.A. No. 198, 2025
v.	:	
BLACKBAUD, INC., Defendant-Below, Appellee.	:	**Appeal from the Superior Court of the State of Delaware, C.A. No. N22C-12-141 KMM (CCLD)**

OPENING BRIEF OF APPELLANTS

PHILLIPS, McLAUGHLIN & HALL, P.A.
Lisa C. McLaughlin (#3113)
1200 N. Broom Street
Wilmington, DE 19806
(302) 655-4200
lcm@pmhdelaw.com

OF COUNSEL:
de LUCA LEVINE LLC
Kenneth T. Levine (*pro hac vice* application forthcoming)
301 E. Germantown Pike, 3rd Floor
East Norriton, PA 19401
(215) 383-0081
klevine@delucalevine.com

Attorneys for Appellants

Dated: June 24, 2025

TABLE OF CONTENTS

TABLE OF CITATIONS

CASES

RULES

NATURE OF PROCEEDINGS

Appellants, Plaintiffs-below,[1] Philadelphia Indemnity Insurance Company ("PIIC"), Acadia Insurance Company ("Acadia"), and Union Insurance Company ("Union"), as subrogees, initiated breach of contract claims against Appellee, Defendant-below Blackbaud, Inc. ("Blackbaud") to recover damages incurred by entities Appellants insured (the "Insureds"). Such damages were caused by Blackbaud's failure to perform obligations owed to the Insureds under the terms of a contract that was the same for each Insured - called the Blackbaud Solutions Agreement (the "BS Agreement") - in connection with a February 7, 2020, ransomware attack on Blackbaud's computer system (the "Data Breach"). Blackbaud specializes in software solutions and online services and databases for educational and nonprofit organizations, and it contracted with the Insureds to provide certain software and online services that enabled the Insureds to collect data and conduct transactions with their donors.

In breach of the terms of the BS Agreements, Blackbaud failed to maintain commercially reasonable cybersecurity protections, enabling the Data Breach. As a result of Blackbaud's failures to perform these contractual duties under the BS Agreement, the Insureds incurred damages, including costs and expenses in

[1] In accord with Supreme Court Rule 14(b)(5), the Appellants will be referred to as "Plaintiffs" through the remainder of the Opening Brief.

connection with investigating and responding to the Data Breach. Subject to any applicable deductibles and other policy terms and conditions, those costs and expenses were covered by insurance policies issued by Plaintiffs each an insurance carrier, which now have contractual and equitable subrogation rights, including recovery rights under the BS Agreements. Plaintiffs seek to recoup those damages that stem directly from the breach of the BS Agreement by Blackbaud.

The court below, addressing a Motion to Dismiss Plaintiffs' operative First Amended Complaint ("Complaint") that stated a *prima facie* claim satisfying all elements for breach of contract and met the minimal pleading standards under applicable Delaware law, inexplicably concluded that the Complaint failed to adequately do so and dismissed the Complaint with prejudice, despite never concluding it would be impossible for Plaintiffs to state a proper claim. Ultimately, this appeal should be resolved based on straightforward application of established principles for what is required to state a claim for breach of contract under Superior Court Civil Rules 8 and 12(b)(6).

SUMMARY OF ARGUMENT

1. The Superior Court erred by holding that Plaintiffs failed to adequately state a claim for breach of contract under the minimal notice pleading requirements of Superior Court Civil Rules 8 and 12(b)(6).

2. In the alternative, the Superior Court erred by dismissing the action with prejudice, as the court never held that Plaintiffs could never state a claim as a matter of law and thus was required to give Plaintiffs the opportunity to amend the Complaint.

STATEMENT OF FACTS[2]

A. THE PARTIES

1. Plaintiffs

Appellant PIIC is a Pennsylvania corporation with its principal place of business located in Bala Cynwyd, Pennsylvania. Appellant Acadia is an Iowa corporation with its principal place of business located in Westbrook, Maine. Appellant Union is an Iowa corporation with its principal place of business located in Urbandale, Iowa. Each Appellant is engaged in the business of, *inter alia*, underwriting insurance, including cyber-related insurance.

The Insureds were and are educational and nonprofit organizations that were all clients of Blackbaud. (A061-67, Op. at 3).

Plaintiffs issued insurance policies to the Insureds, and such policies provide coverage for incidents such as the Data Breach. (A0065 (¶18)). Pursuant to the terms of their insurance policies, Plaintiffs paid amounts covered in excess of the Insureds' retentions for damages incurred as a proximate result of the Data Breach, including, but not limited to, breach coach and counsel fees, computer systems forensic review and recovery, migration services, and notification and credit

[2] The Complaint and Exhibits 1-5 thereto are appended and cited as A0061-0197 (see Appendix), as is the format for all Appendix citations. The Opinion and Order below dated April 3, 2025, is attached hereto as Exhibit A, and cited as "Op.".

monitoring costs to certain customers - which total over $600,000. (A0093-94 (¶¶139-142)). The insurance policies contain subrogation clauses, which provide recovery rights to the extent of coverage payments, including the right to recoup those coverage payments that stem directly from the breach of the BS Agreement by Blackbaud. (A0094 (¶142); Op. at 3). Plaintiffs pursue this breach of contact claim as subrogee of the Insureds.

2. Blackbaud

Blackbaud is a Delaware corporation with its principal place of business in Charleston, South Carolina. Blackbaud is a technical solutions and software company that services educational and/or nonprofit organizations. (A0066 (¶¶ 22)). Blackbaud provided software solutions to the Insureds that enabled them to collect and maintain certain confidential information, including personal identifying information, from their donors. (Op. at 1; A0068 (¶33)). Blackbaud entered into identical BS Agreements with each of the Insureds for the provision of certain Blackbaud solutions and services. (A0067 (¶¶26-28)), Op. at 1).

B. THE BS AGREEMENTS

The BS Agreements governed/govern Blackbaud's relationship with, and the provision of technical solutions, software and services to, the Insureds to assist them

in managing data, collecting payments, and conducting other transactions with donors. (A0067-68 (¶¶28-33)). By using Blackbaud's software and solutions in this manner, the Insureds captured data about donors and other persons that included, *inter alia*, contact information, donation history and payment information, which was stored in Blackbaud's systems and included "protected health information ("PHI") and personally identifiable information ("PII")." (A0068 (¶¶32-33); Op. at 1).

In return, through the BS Agreements, Blackbaud committed to "maintain administrative, physical, and technical safeguards designed to (i) protect against anticipated threats or hazards to the security of Your Confidential Information, and (ii) to protect against unauthorized access to or use of Confidential Information that could materially harm You[,]" and to "at all times maintain commercially reasonable information security procedures and standards." (A0177, §6.a.). The BS Agreements provide that Blackbaud "ha[s] implemented commercially reasonable, written policies and procedures addressing potential Security Breaches and ha[s] a breach response plan in place." (*Id.* §6.b.). Blackbaud further committed that, "[i]n the event of Security Breach, We will use commercially reasonable efforts to mitigate any negative consequences resulting directly from the Security Breach" and would provide notification of any breach to the Insureds within 72 hours. (*Id.* §§6.c.-d.).

The BS Agreements are governed by New York law. (A0177, §14).

C. BLACKBAUD'S CYBERSECURITY FAILURES

As acknowledged in the BS Agreement, Blackbaud was aware that its clients, including the Insureds, were using its software solutions to manage and store confidential information and had made express contractual promises to "protect against anticipated threats or hazards to the security of [the Insureds'] Confidential Information, and (ii) protect against unauthorized access to or use of Confidential Information that could materially harm [the Insureds]." (A0177, §6.a.). Nonetheless, Blackbaud improperly maintained sensitive data on outdated, obsolete and unpatched servers in the face of cybersecurity concerns voiced by its own employees and information security analysts. (A0071 (¶¶46-47)). These practices were inconsistent with Blackbaud's commitment to "at all times maintain commercially reasonable information security procedures and standards[]" and exposed the confidential information of Insureds' donors to cyberattack. (A0177, §6.a.; A0086-87 ¶122).

D. THE DATA BREACH

On February 7, 2020, a hacker gained access to Blackbaud's systems where it remained undetected until May 2020. (A0073 (¶¶57-59). On May 14, 2020, Blackbaud retained Kudelski Security to investigate the Data Breach, and on June 14, 2020, Kudelski Security issued a report finding that Blackbaud did not have

proper cybersecurity measures in place to prevent the hacker from gaining access to Blackbaud's systems, creating administrator accounts, moving around freely in those systems, and exfiltrating confidential information, including that of the Insureds' donors. (A0073-74 (¶¶59-64)). The hacker threatened to publish the stolen data and demanded a ransom, which Blackbaud paid in the amount of twenty-four Bitcoins. (A0075 (¶73)). Blackbaud failed to confirm that the hacker had deleted all the stolen data in exchange for the ransom payment. (*Id.* ¶74).

In connection with the Data Breach, Blackbaud analyzed the exfiltrated files to determine which of its customers and solutions were affected, and concluded that "millions of consumers' full names, age, date of birth, social security numbers, … financial information …, medical information …, employment information (including salary) …, and account credentials" were accessed and exfiltrated. (*Id.* ¶77). Blackbaud's investigation revealed that the hacker "has unauthorized access to and exfiltrated over a million files concerning over 13,000 or roughly a quarter, of Blackbaud's customers, including the Blackbaud Clients," defined in the Complaint as the Insureds and their donors. (A0076 (¶78)). As educational and nonprofit organizations, the Insureds collected confidential information from their students, customers and donors, which was the very purpose of using Blackbaud's software - to assist the Insureds to "manage data about their donors, including identifying information, donation history, and financial information." (A0067 (¶25)). Indeed,

"Blackbaud generates revenues from software solutions …; payment and transaction services; software maintenance and support services; and professional services" that inherently require the payor to enter confidential information into Blackbaud's systems. (*Id.* (¶26)). In other words, Blackbaud was well aware of the types of general confidential information that the Insureds were collecting and storing on Blackbaud's systems - information that was in Blackbaud's custody and care.

On July 16, 2020, Blackbaud issued its first public notice of the Data Breach on its website. (A0076 (¶79)). It informed customers, including the Insureds, that "[t]he cybercriminal did not access credit card information, bank account information, or social security numbers" and that "**[n]o action is required on your end because no personal information about your constituents was accessed**." (*Id.* (¶85)) (emphasis in original). Blackbaud's August 4, 2020 Form 10-Q disclosed the Data Breach but omitted material information about what data was accessed and presented the exfiltration of sensitive donor information as hypothetical. (A0077 (¶89)). That was false, as noted immediately below.

On September 29, 2020, Blackbaud filed a Form 8-K acknowledging that "the cybercriminal may have accessed some unencrypted fields [with] bank account information, social security numbers, usernames and/or passwords." (*Id.* (¶91). The Securities and Exchange Commission (the "SEC") sanctioned Blackbaud on March 9, 2023, for such early misleading disclosure and Blackbaud agreed to pay a penalty

of $3 million to resolve allegations as to disclosures. (A0078 (¶92)). The SEC settlement was followed on October 29, 2023, by resolution of investigations by 50 states attorneys general where Blackbaud paid $49.5 million to address its violations of "state consumer protection laws, breach notification laws, and HIPAA [due to its] fail[ure] to implement reasonable data security and remediate known security gaps … and then failing to provide its customers with timely, complete, or accurate information regarding the breach, as required by law." (A0078-79 (¶¶94-97, and n.16)) (quoting Delaware Attorney General press release). The attorneys' general investigations and settlements confirmed that Blackbaud improperly secured confidential information, including HIPAA-protected data, of its consumers. (A0079-80 (¶98)).

E. THE INSUREDS' INVESTIGATIONS AND RESULTING EXPENSES

After making the inaccurate initial disclosures noted above, instead of completing a full investigation and notifying the Insureds of the nature and scope of data that was exfiltrated, Blackbaud merely passed the buck to the Insureds by providing them with only a "Toolkit" that instructed them as to the necessity to conduct their own independent investigations. (A0094-96 (¶¶145-149). While making misstatements about the Data Breach, the Toolkit directly instructed the Insureds to undertake a list of required "next steps," such as investigating the data

involved, consulting with legal counsel and possibly notifying donors. (*Id.)* As a first step, the Insureds were directed to perform an "initial analysis and investigation …, *irrespective* of what data was later determined to be affected and *irrespective* of what laws were eventually determined by legal counsel to apply to such data." (A0236 (emphasis in original); A0092 (¶139)).

The Insureds' investigations were somewhat frustrated by Blackbaud's inaccurate information about the scope of the Data Breach that went uncorrected for months before Blackbaud confirmed that social security numbers and bank account information were exfiltrated too. (A0104 (¶¶189-191)). In addition, because the information was stored on Blackbaud's systems, not the Insureds' own systems, the Insureds could not effectively or directly investigate the Data Breach themselves. (A0105 (¶194)). In performing these investigations, the Insureds incurred costs and expenses for computer forensic firms, legal counsel to investigate the scope of the Data Breach and any necessary notification requirements, and the costs of notification to certain donors, accordingly. (A0091-94 (¶¶139-140)). Those damages amount collectively to more than $600,000. (A0094 (¶¶141-142).

F. STAGE OF THE PROCEEDINGS

Plaintiffs filed their initial Complaint on December 13, 2022. (A0002; A0014). On January 5, 2023, Blackbaud filed an answer to the initial Complaint,

followed by an amended answer on January 26, 2023. (A0002-0003). On February 13, 2023, Blackbaud filed a Motion to Dismiss and Motion for Judgment on the Pleadings. (A0004). Oral argument was held on January 9, 2024. (A0007). The Superior Court then granted Blackbaud's Motion to Dismiss on March 27, 2024. (*Id.;* A0028, *et seq.*). Plaintiffs filed a Motion for Reargument that was technically denied on April 19, 2024, but in such decision the Superior Court allowed Plaintiffs to amend their initial Complaint. (A0007-0008).

On May 17, 2024, Plaintiffs filed their First Amended Complaint. (A0061, *et seq.*). On June 28, 2024, Blackbaud filed a Motion to Dismiss the First Amended Complaint. (A0008-0009). Oral argument was held on December 13, 2024, and a Transcript of such argument is provided in the Appendix at A0247-371. The Superior Court requested supplemental briefing, which was completed by the parties on January 10, 2025. (A0012; and A0389, *et seq*.). The Superior Court issued its Opinion and Order (the "Opinion" or "Op.," attached hereto as Exhibit "A") dismissing the case *with prejudice* on April 3, 2025.

Plaintiffs timely filed their Notice of Appeal on May 5, 2025. (A400, *et seq.*).[3]

[3] Great American Spirit Insurance Company and Great American Alliance Insurance Company were plaintiffs along with Appellants at the trial level, but are not participating in the appeal.

ARGUMENT

I. THE SUPERIOR COURT ERRED IN FINDING THAT THE COMPLAINT FAILED TO STATE A CLAIM FOR BREACH OF CONTRACT

A. Question Presented

Whether the Superior Court erred by holding that Plaintiffs failed to state a claim for breach of contract despite the minimal notice pleading requirements of Superior Court Civil Rules 8 and 12(b)(6)?

(Preserved at A0216-241; A0280-358; A0369-71; A0400-402).

B. Scope of Review and Legal Standards

1. Appellate Review

The Court's review of the decision on a motion to dismiss under Superior Court Civil Rule 12(b)(6) for failure to state a claim is *de novo*. *Clinton v. Enter. Rent-A-Car Co.*, 977 A.2d 892, 895 (Del. 2009).

When reviewing a ruling on a motion to dismiss, this Court "1) accept[s] all well pleaded factual allegations as true, (2) accept[s] even vague allegations as 'well pleaded' if they give the opposing party notice of the claim, (3) draw[s] all reasonable inferences in favor of the non-moving party, and (4) [does] not affirm a dismissal unless the plaintiff would not be entitled to recover under any reasonably

conceivable set of circumstances." *Cent. Mortgage Co. v. Morgan Stanley Mortg. Cap. Hldgs LLC*, 27 A.3d 531, 535 (Del. 2011).

This Court has similarly observed that "[i]n reviewing the grant or denial of a motion to dismiss, we view the complaint in the light most favorable to the non-moving party, accepting as true its well-pled allegations and drawing all reasonable inferences that logically flow from those allegations." *Clinton*, 977 A.2d at 895.

2. Pleading Standards

To plead a claim under Superior Court Civil Rule 8(a), a plaintiff must merely provide "(1) a short and plain statement of the claim showing that the pleader is entitled to relief and (2) a demand for judgment for the relief to which the party deems itself entitled." Under this notice pleading standard in Delaware, "for a complaint to survive a motion to dismiss, it need only give 'general notice of the claim asserted.'" *Doe v. Cahill*, 884 A.2d 451, 458 (Del. 2005). "A complaint that gives fair notice 'shifts to the [opposing party] the burden to determine the details of the cause of action by way of discovery for the purpose of raising legal defenses.'" *Wellgistics, LLC v. Welgo, Inc.,* 2024 WL 4327343, at *7 (Del. Super. Sept. 27, 2024) (Miller, J.) (quoting *VLIW Tech., LLC v. Hewlett-Packard Co.*, 840 A.2d 606, 611 (Del. 2003)).

As the Superior Court itself acknowledged in this case, to adequately plead a breach of contract claim, as to the initial element "[a] party must identify the particular contractual terms that were breached.'" (Op. at 19) (quoting *Marydale Preservation Assoc., LLC v. Leon N. Weiner & Assoc., Inc.*, 2022 WL 4446275, at *17 (Del. Super. Sept. 23, 2022)). Damages, though, "may be pled **generally**," and a party merely must "allege facts raising a **reasonable inference** that damages are causally related to the alleged misconduct." *Spring League, LLC v. Frost Brown Todd LLP*, 2024 WL 4442006, at *2 (Del. Super. Oct. 8, 2024) (emphases added) (citations omitted).

Dismissal is appropriate only where it "appears with reasonable certainty that, under any set of facts that could be proven to support the claims asserted, the plaintiff would not be entitled to relief," *Clinton*, 977 A.2d at 895; and an allegation, "'though vague or lacking in detail' can still be well-pleaded so long as it puts the opposing party on notice of the claim brought against it." *Doe*, 884 A.2d at 458. "[A] trial court **must** draw all reasonable factual inferences in favor of the party opposing the motion." *Id.* (emphasis added).

To avoid dismissal under Delaware's notice pleading standard, a party "need not plead evidence," but instead must merely "allege facts that, if true, state a claim upon which relief can be granted." *Wellgistics, LLC v. Welgo, Inc.*, 2024 WL 4327343, at *7 (quoting *VLIW Tech., LLC,* 840 A.2d at 611).

C. Merits of Argument

The Superior Court correctly observed that under New York law (which substantively governs the terms of the BS Agreements), "[t]o 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.'" (Op. at 19) (citation omitted).

The Superior Court's own recitation of the alleged facts established for each Insured the existence of a contract, breach of each such contract, and damages resulting from each such breach - in other words, a *prima facie* claim for breach of contract for each Insured individually, and Plaintiffs collectively, that satisfies the requirements of Rules 8 and 12(b)(6).

The court itself appeared to recognize the veracity and simplicity of these pleading standards during the oral argument on Blackbaud's Motion to Dismiss, stating: "[T]hey have enough to state a claim. It was a contract, there was a breach, we had damages. The amount of the damages and then, ultimately, whether they all are, the whole category is proximate cause, figure that out through discovery." (A0364-365).

Despite this clarity in the pleadings, and in the Superior Court's apparent understanding and recitation of Plaintiffs' allegations, the court inexplicably reached the wrong decision in the end, erroneously finding that Plaintiffs failed to adequately

assert claims for breach of contract despite Delaware's liberal pleading standards. (Op. at 3). The reasons for this strange digression from these simple logical steps are hard to understand, and hard to follow at times.

As set forth below at great length, it appears that the Superior Court failed to draw all reasonable factual inferences in Plaintiffs' favor, as it was required to do, and improperly held Plaintiffs to a higher pleading standard than required for pleading a breach of contract. This was done as to two different overarching considerations of Plaintiffs' claims: (1) the court erroneously concluded that the Complaint impermissibly aggregated the Insureds' claims together instead of providing additional separate allegations for each, and (2) relatedly, it erroneously concluded that the Complaint's allegations as to proximate cause are "conclusory" rather than well-pled. (*Id.* at 2-3*).* Both findings were simply wrong and held Plaintiffs to a higher pleading standard than required under Delaware law. *See* Super. Ct. Civ. R. 8(a); *Spring League*, 2024 WL 4442006, at *2; *Doe*, 884 A.2d at 458.

The Complaint has well-pled, non-conclusory allegations as to the existence of a contract, breach of that contract, and damages resulting from that breach - for ***each*** Insured - and that are sufficient to place Blackbaud on notice of the claims asserted against it and Plaintiffs' theory of damages – as to ***each*** Insured.

1. The Complaint Adequately Alleges the Existence of a Contract for Each Insured

As to the first element of the breach of contract claim, the Superior Court acknowledged, regarding the BS Agreements, that "[e]ach Insured entered into a separate 'Solutions Agreement' with Blackbaud (the 'Contracts'). Under the Contracts, Blackbaud provided subscriptions and services relating to its software products." (Op. at 4) (citation omitted). The Superior Court similarly acknowledged that under such BS Agreements "Blackbaud was contractually required to safeguard 'Confidential Information' (defined to include: '(iii) donor, student, prospect and financial information') using "'commercially reasonable' cybersecurity procedures." (*Id*.). As the Court noted, Section 6 of the BS Agreements provided:

> a. We 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**....

(*Id*.) (emphasis added).

There were two <u>additional and separate</u> contractual provisions that Plaintiffs alleged were also breached: (a) Blackbaud committed to notify the Insureds within 72 hours and (b) Blackbaud was required "use commercially reasonable efforts to mitigate any negative consequences resulting directly from" any data breach, whether or not it was caused by Blackbaud. (Op. at 4-5) (quoting from A0177

(§6.d.)). Plaintiffs mention these additional contractual provisions simply because the Superior Court, as noted below, clearly focused at pivotal times on the latter additional contractual provision (the duty to mitigate) to the exclusion of the principal contractual provision that Plaintiffs alleged was breached: to safeguard 'Confidential Information' using commercially reasonable cybersecurity procedures.

2. The Complaint Adequately Alleges a Breach of Contract for Each Insured

As to the second element of a breach of contract claim, the Superior Court observed that: "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." (Op. at 15) (citation omitted). The court further described :

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

(*Id.* at 27) (emphases added; citations omitted).

Earlier, the court had noted and described Plaintiffs' well-pled allegations under the heading "***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. The older servers were not on a routine maintenance schedule, so security updates were not implemented. Failure to run security patches on these older servers concerned Blackbaud employees.
>
> Additionally, a former information security analyst warned Blackbaud about process vulnerabilities in its systems. 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.'" 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. Blackbaud knew the risk was so high that employees would "simply shut down certain machines at times." 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 ...." Blackbaud also failed to require customers to encrypt social security numbers and bank account information stored in certain fields on the system.
>
> Finally, Blackbaud retained some current and former customers' data for years longer than needed, unnecessarily exposing this data to a cyber breach.

(*Id.* at 11-13) (citing numerous provisions in the Complaint).

The Complaint specifically alleges that: "By failing to implement such proper and commercially reasonable encryption practices, Blackbaud allowed the Incident

to occur and breached the [BS Agreements]." (A0084 (¶115; *see also id.* ¶¶172.d., 180). This allegation was supported by the Delaware Attorney General's own conclusions alleged in the regulatory settlement with Blackbaud, and that were quoted by the Superior Court below:

> 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.

(Op. at 10) (quoting A0078 (¶94)) (emphasis added).

The foregoing allegations are clearly sufficient to state a claim for breach of contract as to each Insured, as such factual assertions would each act as a material breach of the explicit contractual duties noted above to safeguard "Confidential Information" using commercially reasonable cybersecurity procedures - affecting all Insureds in the manner noted above and detailed below.

3. The Complaint Adequately Alleges Damages Suffered by Each Insured that were Proximately Caused by the Breaches of Contract

As to damages, the Superior Court perfectly summarized the Complaint's allegations that "[t]he Insureds incurred expenses to investigate and comply with

their obligations under applicable laws," that flowed directly from the underlying computer system compromise (Op. at 13):

> Collectively, the expenses included: (i) 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"). These Expenses were paid by the applicable Plaintiff, except to the extent that the policy contained a deductible.

(*Id.* at 13-14) (citing A0091-93 (¶¶139-141).[4]

The Superior Court recognized that the Complaint represents that each Insured undertook and incurred the expenses of such investigative steps in direct response to Blackbaud's computer system compromise – and in accord with Blackbaud's own

[4] While Plaintiffs' Complaint identified each underlying Insured, and this precise list of damages caused by the computer compromise, Plaintiffs admittedly did not provide a specific dollar breakdown for each Insured in the body of the Complaint, but expected to do so in response to any possible Rule 9(g) request. Under such rule, any "pleading ... which prays for unliquidated money damages, shall demand damages generally without specifying the amount…. Upon service of a written request by another party, the party serving such pleading shall, within 10 days after service thereof, serve on the requesting party a written statement of the amount of damages claimed." Super. Ct. Civ. R. 9(g). Any absence of dollar amount allegations on an Insured-by-Insured basis as to each Insured's damages was not noted as a basis for dismissal, and a lack of specific dollar amount pleading by a Plaintiff has never been identified under Delaware law as a basis for dismissal. *Id*.

instructions in the form of the "Toolkit" it sent to its customers to address the data breach:

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

(Op. at 8) (first emphasis in original, latter emphases added) (citing A0185, Step 2 of the Toolkit Instructions).

As the Superior Court further noted: "Plaintiffs point to the Toolkit as Blackbaud 'admit[ting]' that remediation expenses, such as the Expenses, were a

necessary result of the data breach." (Op. at 16). "[T]he Toolkit 'instructed' Insureds to consult with legal counsel, [and] determine what laws applied to them," and "'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." (*Id*.) (citing A0095 (¶¶149-155). (*See also* Op. at 26 ("[E]ach [Insured] was forced to conduct its own investigation, as the Toolkit suggested.")). As admitted within the Toolkit instructions, the Insureds were each legally compelled to incur these damages regardless of the types of data they were in fact storing within Blackbaud's systems. Until such investigative expenses were incurred, the type of data stored on the vulnerable portions of Blackbaud's system could never be identified, and any legal decisions as to future notification requirements could not be properly analyzed.

The Complaint identified those exact damages and how they were proximately caused by the breach: "Blackbaud Clients had obligations to their respective Consumers to protect confidential information and were forced to undertake independent investigations into the Incident to meet their legal obligations to investigate and notify affected Consumers (the "Remediation Expenses")." (A0081 (¶104)). It further alleges that: "Plaintiffs and the Blackbaud Clients have suffered damages (*i.e.*, the Remediation Expenses) because of Blackbaud's well

documented failure to uphold its contractual obligations under the [BS Agreement] …." (*Id.* (¶107)).

The Complaint also details the types of Remediation Expenses incurred by the Insureds:

> Because of the Incident, Blackbaud's breaches of contract, and the applicable laws and regulations, the Blackbaud Clients were forced to incur Remediation Expenses to comply with the Blackbaud Clients' legal obligations in the wake of the Incident and Blackbaud's failures, including:
>
> a. Retention of outside counsel to identify, assess, and comply with the legal obligations triggered by the Incident under laws and regulations;
> b. Retention of computer forensic experts to investigate the Incident, because of Blackbaud's failure to do so and accompanying misrepresentations, as required under laws and regulations;
> c. Retention of outside counsel and print vendors to draft, translate, print, and mail letters under laws and regulations, or to undertake such work themselves;
> d. Retention of vendors to respond to third-party inquiries, such as regulators and Consumers; and/or
> e. Incurring of other expenses as required under laws and regulations.

(A0094 (¶140)). A detailed explanation for the bases for undertaking these expenses, and the flowchart of necessary steps to be undertaken after the Data Breach occurred is provided in Paragraph 139 of the Complaint and clearly provides the nexus between the data Breach and the damages above. (A0091-93 (¶139). Additionally, as the court itself recognized, Plaintiffs' Complaint included a

detailed list of the Insureds (all Blackbaud's customers), identifying their name and principal location. (Op. at 15).

The Superior Court at oral argument seemed to have fully understood the nature of the damages incurred by each Insured and how they were proximately caused by the Data Breach:

> THE COURT: … these insureds, once they got the notice of the data breach, they had an obligation to investigate to know what other obligations they may have had. So it doesn't matter what state laws some of them may have had to comply with regard to notice, they all did this investigation, and that's where it starts. They wouldn't have had to have done this investigation had there not been a breach of the contract by this data breach occurring, which was alleged to be an at-fault breach. It flows right after. They wouldn't have had to have done it. Blackbaud is alleged to have not lived up to the commercially reasonable standard. Why is it then that the allegation that we had to incur these because that data breach occurred sufficient?
>
> MS. HUTCHINS: Your Honor, I would first say, again, the pleading is not sufficient to even tell us if they had to do that investigation. Name and address, for example, if that's all that was provided by an insured, wouldn't trigger that.
>
> THE COURT: Well, they don't know. The notification is different. They're not saying -- as I'm understanding their argument today, there's a data breach, Blackbaud told us, and insured gets this. What do we have to do? Do I even have to notify anybody? So they go to their lawyer and say, "Got this breach. Here's the information we have. What do I have to do?" The lawyer that researches it all could come back and say, "You know what, you didn't have that data so you don't have to give any notification." But the insured incurred the expense to make that determination, and it would not have had to have done that had there not been the data breach.

(A0360-361).

Thus, fairly read and with all reasonable inferences being drawn in Plaintiffs' favor, the Complaint alleges the identities of each Insured, and the types of expenses incurred by the Insureds as a result of Blackbaud's breach of the BS Agreements. These allegations are sufficient to provide general notice to Blackbaud of the damage claims asserted against it and how they were proximately caused by the breach, and there is simply no need for further detail at the pleading stage under Delaware's liberal notice pleading requirements.[5]

4. Superior Court Erred by Holding that Plaintiffs Failed to Adequately State Claim under Minimal Notice Pleading Requirements

Despite all the acknowledgements noted about as to the nature and sufficiency of the claims asserted, the Superior Court inexplicably held that Plaintiffs failed to adequately plead their breach of contract claim.

---

[5] To the extent that the Superior Court was of a belief, however mistaken, that in the Complaint Plaintiffs needed to further break down the specific damages incurred by each Insured, then it should never have dismissed the Complaint *with prejudice*. The Court was well aware, as noted in footnote 86 to the Court's Opinion, that prior to suit Blackbaud had already been provided with the scope and extent of each Insureds' damages claims, and the invoices and receipts in support of such damages. While such specific details were not included in the Complaint as wholly unnecessary, if the Court felt otherwise, Plaintiffs could certainly have further amended their pleadings to refer to and attach the hundreds of pages of detailed supports for each Insured's damages.

a. Insured-Specific Facts

The Court concluded that the Complaint failed to state a claim because it did "not allege Insured-specific facts." (Op. at 21). As noted above, though, the Court had acknowledged that each Insured had the same contract, and that a breach of the duty to maintain commercially reasonable cybersecurity measures would be a breach of such contractual provision in each Insured's contract. The Court also acknowledged that it was alleged in the Complaint that each Insured had suffered investigative expenses, and possibly additional notification expenses, as a result of the breach of such common contractual requirement.

Nonetheless, the Court, without ever explaining why an additional level of detail was necessary under Delaware's notice pleading standard, identified a few areas that it felt required more detail for each Insured:

- "[Plaintiffs] allege that the Insureds investigated what data they stored, but do not identify the data stored by each." (Op. at 21).
- "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." (*Id.)*
- "[Plaintiffs] do not allege what privacy law requirements any Insured allegedly had to satisfy," and "The amended complaints do not allege which, if any, of the listed laws applied to each Insured." (Op. at 22).
- "[Complaint does] not include Insured-specific factual allegations of the type(s) of Expenses allegedly incurred." (Id.)

The Court further noted that "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." (Op. at 22). This is simply inexplicable substantively (or under Delaware's notice pleading standards) how the absence of these extra facts (especially when they are to be viewed in the light most favorable to Plaintiffs) could ever affect the validity of Plaintiffs' claims.

As to the first three purported deficiencies, none of them have any bearing whatsoever on whether a proper breach of contract claim was adequately asserted, collectively or as to individual Insureds. As alleged in the Complaint, and highlighted repeatedly above, as soon as notice of the data breach occurred **each Insured had to incur costs to investigate (forensically and legally)** the type of data stored on the Blackbaud servers, and whether any privacy laws compelled further notification based upon those findings. This is also exactly what Blackbaud in its Toolkit directed each Insured to do. Whatever characteristics the data eventually was identified to have, and whether or not one or more of the various state privacy laws were then found to be violated, has no bearing on the adequacy of the Plaintiffs' pleadings. These purported deficiencies merely demonstrate that the Superior Court lost its way as to the nature of the Insureds' common damages that arose from the Blackbaud computer compromise: the need for all Blackbaud customers to undertake expensive investigations as to the nature of the data and as to any privacy law violations. In turn, such additional factual allegations would have

no bearing on the adequacy of Plaintiffs' pleadings, or similarly whether Blackbaud could "assess whether the subrogor-Insureds have a valid claim."

Similarly, the Court's requirement that Plaintiffs' Complaint include "Insured-specific factual allegations of the type(s) of Expenses allegedly incurred" is also without basis, both legally under Delaware pleading law or factually in this case. As noted above, the types of common expenses incurred by the Insureds were detailed in the Complaint and all involved investigative expenses, and some additional notification expenses for certain Insureds. This is true as to the pleading standards whether there was one Insured or hundreds of Insureds. Under Delaware law damages "may be pled generally" and a party merely must "allege facts raising a reasonable inference that damages are causally related to the alleged misconduct." *Spring League,* 2024 WL 4442006, at *2. There are no further pleading requirements as to damages, and such a standard is certainly met here. The obvious analogy here is to a bus full of individuals who suffered damages because of a single accident. Such collective plaintiffs just would need to plead that they incurred resultant "medical expenses," but would not need to go into detail in their collective complaint as to which ones had head injuries, which ones had to pay for physical therapy, and which ones had permanent injuries. Moreover, if the details as to the individual Insured's expenses were actually dispositive (which they were not), then the Superior Court could simply have dismissed the Complaint without prejudice, and directed Plaintiffs

to amend so as to add the detailed Insured-by-Insured breakdown that Blackbaud already possesses (as noted in footnote 5 above).

There is no support under Delaware law for the Superior Court's imposition of any higher pleading standard requiring Plaintiffs to plead any more precise Insured-by-Insured claims with factual particularity. (*See* Op. at 22-25). The Superior Court strangely relied on three New York cases cited by Blackbaud for the court's conclusion that Plaintiffs had failed to adequately plead a claim under Delaware law, quoting "'[a]t the very least,' … plaintiffs were required to identify subrogors '*and those subrogors' claims so that defendants would have the opportunity to assert defenses against those claims.*'" (Op. at 23) (quoting *Blue Cross & Blue Shield of N.J., Inc. v. Philip Morris USA Inc.*, 344 F.3d 211, 218 (2d Cir. 2003); *A.O. Fox Mem'l Hosp. v. Am. Tobacco Co., Inc.*, 754 N.Y.S.2d 368, 414 (N.Y. App. 2003)) (emphasis in original); *see Id.* at 23, n.79 (quoting *Blue Cross*, 344 F.3d at 217-18; *A.O. Fox Mem'l Hosp.*, 754 N.Y.S.2d at 414; *E. States Health & Welfare Fund v. Philip Morris USA Inc.*, 719 N.Y.S.2d 240 (N.Y. 2000)). Plaintiffs did identify all affected Insureds in their Complaint, and nothing in those decisions based upon New York pleading standards even actually require a plaintiff "to separately plead the claims of each Insured, supported by Insured-particular facts." (Op. at 25).

Moreover, those cases were distinguished by New York's highest court in the *Lawyers' Fund For Client Protection of State of New York v. JP Morgan Chase Bank, N.A.,* 915 N.Y.S.2d 741 (N.Y. App. 2011), which observed that "the claims in those cases were dismissed not merely because the injured persons had not been identified, but because they could not be identified in a manner appropriate to a subrogation claim." 915 N.Y.S.2d at 743 (citing *Blue Cross*, 344 F.3d at 217-18; *A.O. Fox Mem'l Hosp.*, 754 N.Y.S.2d at 368; *E. States Health & Welfare Fund*, 719 N.Y.S.2d at 240). In those cases, "[t]he separate claims asserted on behalf of the injured persons involved such a high degree of individualized inquiry that … they '[could not] properly be considered to be subrogated.'" *Lawyers' Fund*, 915 N.Y.S.2d at 743. In *Lawyers' Fund* the court held instead "that plaintiff's original complaint provided defendant with notice of the facts, transactions and occurrences to be proven" because it "stated the number of claimants, the time frame within which their losses occurred, and the **aggregate** amount of their damages, and that, after being reimbursed, the subrogors each signed an agreement transferring their claim to plaintiff." *Id.* (emphasis added). In finding that the motion to dismiss the amended complaint in *Lawyers' Fund* was properly denied, that court found, much like the facts here, that "[e]ach claimant was injured in the same way, each claimant's subrogation relationship to plaintiff arose in the same way, and the specific acts and

omissions by defendant which were alleged to have caused claimants' losses were the same." *Id.*

Overall, there was no need for any greater detail to be provided on an Insured-by-Insured basis for Plaintiffs to adequately plead their breaches of contract in this case; and the Superior Court erred when it decided otherwise.

b. Proximate Cause

The Superior Court also determined that the Complaint failed to adequately allege a proximate causation linking the Insureds' expenses (i.e., damages) to the breach of the BS Agreements. (Op. at 25-32).

This is a strange and baseless conclusion to reach considering the numerous allegations in the Complaint (with support from Blackbaud's own Toolkit guidance) that the Data Breach that arose from the breach of the contractual requirement to provide commercially reasonable security, and that the Insureds incurred expenses because of such incident.

This is a strange conclusion because the Superior Court itself at oral argument succinctly explained the proximate causation allegations to defense counsel, as reflected in the transcript portion quoted above on page 26 of this Opening Brief (citing A0360-361).

This is a strange conclusion because there clearly would have been no basis at all for the numerous Insureds to each incur such investigative and legal expenses if not for the Data Breach, which Plaintiffs clearly alleged arose from the contractual breach.

To get to this strange conclusion, the Court notes that "a plaintiff must provide a factual basis for proximate cause." (Op. at 26) (citing *Wellgistics, LLC v. Welgo, Inc.*, 2024 WL 113967, at *5 (Del. Super. Jan. 9, 2024)). Plaintiffs agree with this proposition and cite it themselves above. As noted repeatedly above, Plaintiffs' Complaint provided a simple and clear factual basis: contractual breach of security standards caused Data Breach which caused investigative and notification expenses.

Instead of remembering this simple connection from its own statements at the oral argument, the Court appears to have conflated separate contractual obligations in its analysis. Specifically, and without citation to the record, the court wrongly asserted that: "To link the Expenses to the Contracts, Plaintiffs rely on Blackbaud's contractual promise to mitigate the impact of a data breach." (*Id*. at 26). This is not Plaintiffs' argument at all. Blackbaud's contractual mitigation obligations appear in Section ***6.d.*** of the BS Agreements. (*Id*. at 5). These are <u>separate</u> obligations from Blackbaud's promise under Section. ***6.a.*** to "maintain commercially reasonable information security procedures and standards." As the court noted elsewhere, "[i]f a Security Breach occurred due to Blackbaud's failure to maintain this level of

security, it would breach the Contract." (Op. at 27). That is precisely what the Complaint repeatedly alleges, as well as how the damages flowed from Blackbaud's failure to maintain commercially reasonable information security procedures and standards. (*see, e.g.,* A0069 (¶36); A0074 (¶69); A0101 (¶182)).[6]

Similarly, in the latter portion of the Opinion, the Superior Court also conflates other issues with the simple proximate cause analysis, and at times states inaccurate "straw man" responses by Plaintiffs that are and were not actually Plaintiffs' positions. For example, the Court starts out Section V.C. of the Opinion by noting a Blackbaud argument that the Complaint contains "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." (Op. at 25). This issue as to the actual data of each Insured, and whether or not its existence would require further action by Plaintiffs' Insureds, was negated above, and Plaintiffs have explained repeatedly why each Insured had to take certain actions at their expense

[6] To be clear, Plaintiffs do also allege that Blackbaud breached its mitigation obligations. But that separate alleged breach is unnecessary for Plaintiffs to plead that Blackbaud's failure to maintain commercially reasonable information security procedures and standards resulted in damage. It is also unnecessary for this Court to opine on the adequacy of Plaintiffs' additional allegations regarding Blackbaud's breach of its mitigation obligations because the allegations that Blackbaud failed to maintain commercially reasonable security protections are sufficient to reverse the Superior Court's dismissal of the Complaint.

after receiving notice of the Data Breach (and how they were instructed to do so in Blackbaud's own Toolkit).

Instead of considering and accepting such simple position, the Court misstates Plaintiffs' responsive position and noted that "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." (Op. at 26). This was not Plaintiffs' position and instead conflated extra and separate allegations that Blackbaud was untruthful throughout its post-incident reporting. While such allegations are accurate, and affected certain Insureds, Plaintiffs had properly pled that their damages were proximately caused by Blackbaud separate and apart from such additional poor conduct on Blackbaud's part.

The Court repeated this exact same misstatement later in its Opinion to start the section entitled "3. Plaintiffs' Conclusory Cause Allegation are (sic) Insufficient." (Op. 31). The Court again errs there when its states: "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." (*Id.*). This was again simply an inaccurate statement of Plaintiffs' position and allegations. More accurately, Plaintiffs asserted that the investigative and other remediation expenses were proximately caused by

the computer compromise caused by Blackbaud's failure to employ commercially reasonable security measures.

The Superior Court seems to have simply lost its way in the face of an ever-expanding list of extraneous arguments made by Blackbaud demanding additional facts beyond those provided, which placed Blackbaud on notice of the substantive claims asserted against it. Plaintiffs' Complaint adequately alleged all necessary elements of the breach of contract claims, and the Complaint should not have been dismissed.

II. IN THE ALTERNATIVE, THE SUPERIOR COURT ERRED BY DISMISSING THE COMPLAINT WITH PREJUDICE

A. Question Presented

Whether the Superior Court erred by dismissing the action with prejudice, despite identifying certain additional information that if included would have made the allegations in Plaintiffs' Complaint adequate?

(Preserved at A0209, A0242, A0399 at n.3).

B. Scope of Review and Legal Standard

The Court's review of the decision to dismiss this action with prejudice is *de novo*. *See Gifford v. 601 Christiana Invs., LLC*, 158 A.3d 885 (Del. 2017) ("This Court reviews a trial judge's interpretation of its procedural rules *de novo*."). Leave to amend "shall be freely given where justice so requires." Super. Ct. Civ. R. 15(a).

C. Merits of Argument

In the alternative, any dismissal based upon the Superior Court's expressed reasoning should have been *without prejudice*, as Plaintiffs requested in response to the Motion to Dismiss. (A0209, A0242).

Leave to amend "shall be freely given where justice so requires." Super. Ct. Civ. R. 15(a). *See also Hart v. Parker*, 2021 WL 4824148, at *3 (Del. Super. Oct. 15, 2021) ("leave to amend should be freely given unless there is evidence of undue delay,

bad faith, or dilatory motive on the part of the movant, repeated failure to cure deficiencies, prejudice, futility, or the like.").

The Superior Court did not engage in any analysis before erroneously holding at the end of its decision that, "[b]ecause this was Plaintiffs' second attempt to adequately plead their claims, the amended complaints are ***dismissed with prejudice***." (Op. at 34) (emphasis in original). Putting aside whether the Complaint's allegations adequately satisfy the applicable pleading standards, the court did not find that Plaintiffs would never be able to satisfy them if given the opportunity to amend. Indeed, the premise of the Opinion is that the Complaint failed to provide non-conclusory facts regarding the separate damages suffered by each Insured - ***not*** that the alleged damages are unrecoverable as a matter of law. To the contrary, the court observed that "[i]f a Security Breach occurred due to Blackbaud's failure to maintain [a commercially reasonable] level of security, it would breach the Contract." (Op. at 27). Even if on appeal this Court does not see the unduly restrictive nature of the Superior Court's decision, at the very least Plaintiffs should have been given the opportunity to amend their Complaint to provide the limited additional information that the Court said was missing, which Plaintiffs requested in their Answering and Supplemental Briefs.

The court's dismissal of the Complaint *with prejudice* seemingly proceeded in accordance with the approach under Court of Chancery Rule 15(a)(5)(b) (formerly

Rule 15(aaa)), but the Superior Court lacks any such rule. Under the circumstances, the Superior Court's dismissal of the Complaint with prejudice - and without elaboration - was error and reversible.

CONCLUSION

For all of the foregoing reasons, the Court should reverse the ruling below.

Respectfully submitted,

/s/ Lisa C. McLaughlin
Lisa C. McLaughlin (#3113)
PHILLIPS, McLAUGHLIN
& HALL, P.A.1200 N. Broom Street
Wilmington, DE 19806
(302)655-4200
lcm@pmhdelaw.com
tlg@pmhdelaw.com

OF COUNSEL:
de LUCA LEVINE LLC
Kenneth T. Levine
(admitted *pro hac vice*)
301 E. Germantown Pike, 3rd Floor
East Norriton, PA 19401
(215) 383-0081
klevine@delucalevine.com

Attorneys for Appellants and Plaintiffs-Below, Philadelphia Indemnity Insurance Company, Acadia Insurance Company, and Union Insurance Company