EFiled: Jun 12 2025 02:54PM EDT
Filing ID 76450525
Case Number 193,2025

IN THE SUPREME COURT OF THE STATE OF DELAWARE

TRAVELERS CASUALTY AND SURETY COMPANY OF AMERICA,	:	
Plaintiff-Below/Appellant,	:	C.A. No. 193,2025
v.	:	
BLACKBAUD, INC.,	:	**Appeal from the Superior Court of the State of Delaware, C.A. No. N22C-12-130 KMM (CCLD)**
Defendant-Below, Appellee.	:	

OPENING BRIEF OF APPELLANT TRAVELERS CASUALTY AND SURETY COMPANY OF AMERICA

HEYMAN ENERIO
GATTUSO & HIRZEL LLP
Kurt M. Heyman (# 3054)
Gillian L. Andrews (# 5719)
222 Delaware Avenue, Suite 900
Wilmington, DE 19801
(302) 472-7300
Attorneys for Plaintiff-Below/ Appellant Travelers Casualty and Surety Company of America

Dated: June 12, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

RULES

NATURE OF PROCEEDINGS

Appellant Travelers Casualty and Surety Company of America ("Travelers"), as subrogee and/or assignee, initiated a breach of contract action against Appellee Blackbaud, Inc. ("Blackbaud") to recover damages incurred by entities insured by Travelers (the "Insureds"), due to Blackbaud's failure to perform obligations owed to the Insureds under the terms of identical Blackbaud Solutions Agreements (the "Contracts"), in connection with a February 7, 2020 ransomware attack at Blackbaud (the "Data Breach"). Blackbaud specializes in software solutions and services for educational and nonprofit organizations and contracted with the Insureds to provide certain software solutions that enabled the Insureds to collect data and conduct transactions with their donors.

In breach of the terms of the Contracts, Blackbaud failed to maintain commercially reasonable cybersecurity protections, enabling the Data Breach. As a result of Blackbaud's failures to perform these duties under the Contracts, the Insureds incurred damages, including costs and expenses in 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 Travelers. In addition to its equitable subrogation rights, most of the Insureds assigned their recovery rights, including any recovery rights under the Contracts, to Travelers. Travelers seeks to recoup from

Blackbaud those damages which stem directly from Blackbaud's breach of the Contracts.

The court below, after faithfully and carefully setting forth the factual allegations and terms of the applicable Contracts demonstrating that Travelers' operative First Amended Complaint and Jury Demand (the "Complaint") states a *prima facie* claim satisfying all the elements for breach of contract and meeting the minimal pleading standard under applicable Delaware law, reaches the surprise—and erroneous—conclusion that the Complaint fails to do so. Compounding the error in this unexpected denouement, the court below dismissed the Complaint ***with prejudice***—without elaboration and despite never concluding that it would be impossible for Travelers to state a claim as a matter of law. 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 Travelers failed to 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. Because the court did not hold that Travelers could not state a claim as a matter of law, at a minimum, it should have given Travelers the opportunity to amend.

STATEMENT OF FACTS[1]

A. THE PARTIES

1. Travelers

Travelers is a Connecticut corporation with its principal place of business located in Hartford, Connecticut, that is engaged in the business of, *inter alia*, underwriting insurance.

The Insureds are 78 educational and nonprofit organizations that were clients of Blackbaud. (*See* A0188-89; Op. at 3).

Travelers issued insurance policies to the Insureds that provide coverage for incidents such as the Data Breach. (A0069 (¶9)). Pursuant to the terms of those insurance policies, Travelers paid amounts covered in excess of the Insureds' retentions for damages incurred as a direct and proximate result of the Data Breach, including, but not limited to, credit monitoring services and call centers, breach coach and counsel fees, computer systems review and recovery, data recovery, and migration services, which total over $1.5 million. (A0069-70 (¶¶10-11)). The insurance policies also contain subrogation clauses, and Travelers obtained assignments of most of the Insureds' recovery rights, including any such rights under

[1] The operative Complaint and Exhibits 1-6 thereto are appended and cited as A0067-216. (*See* Appendix). The Opinion and Order dated April 3, 2025, is attached as Exhibit A, and cited as "Op.".

the respective Contracts, in connection with paying the Insureds' claims. (A0068, A0070 (¶¶5,12); Op. at 3). Travelers pursues this breach of contact claim as subrogee and assignee of those 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. Blackbaud provided software solutions to the Insureds that enabled them to collect and maintain certain confidential information, including payment information, from their donors. (Op. at 1; A0071 (¶¶16-17)). Blackbaud entered into identical Contracts with each of the Insureds for the provision of certain Blackbaud solutions and services. (A0071-72 (¶ 19), A0190-95; Op. at 1).

B. THE CONTRACTS

The Contracts 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. (A0071 (¶¶16-17)). 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. (*Id.*). "Blackbaud provided the [I]nsureds software solutions

to manage their donor's personal identifying information, among other things." (Op. at 1; *see also* A0071 (¶16)).

In return, through the Contracts, 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." (A0192 §6.a.). The Contracts 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 Contracts are governed by New York law. (A0194 §14).

C. BLACKBAUD'S CYBERSECURITY FAILURES

As acknowledged in the Contracts, 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]." (A0192 §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. (A0076-78 (¶¶35-43, 48-49)). 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. (A0192 §6.a.; A0077 (¶43)).

D. THE DATA BREACH

On February 7, 2020, a hacker gained access to Blackbaud's systems where it remained undetected until May 2020. (A0078 (¶¶50-51)). 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. (A0079 (¶¶53-57)). The hacker threatened to publish the stolen data and demanded a ransom, which Blackbaud paid in the amount of twenty-four

Bitcoins. (A0080 (¶66)). Blackbaud failed to confirm that the hacker had deleted all the stolen data in exchange for the ransom payment. (*Id.* (¶67)).

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. (A0081-82 (¶¶69-70)). 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]." (*Id.* (¶71)). As educational and nonprofit organizations, the Insureds collected confidential information from their donors, which was the very purpose of using Blackbaud's solutions to assist the Insureds in "manag[ing] data about their donors, including identifying information, donation history, and financial information." (A0071 (¶16)). Indeed, "Blackbaud generates revenues from software solutions …; [and] payment and transaction services[]" that inherently require the payor to enter confidential information into Blackbaud's systems. (*Id.* (¶17)). In other words, Blackbaud was well aware of the types of 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 that informed its 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**.'" (A0082-83 (¶¶72, 75, 78)) (emphases 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. (A0083-84 (¶82)). That was false.

On September 29, 2020, Blackbaud filed a Form 8-K acknowledging that "the cybercriminal may have accessed some unencrypted fields intended for bank account information, social security numbers, usernames and/or passwords." (A0083-84 (¶83)). That course-correction was sanctioned by the Securities and Exchange Commission (the "SEC") on March 9, 2023, when Blackbaud agreed to pay a penalty of $3 million to resolve allegations that it made misleading disclosures about the Data Breach. (A0084 (¶85)). The SEC settlement was followed on October 29, 2023, by resolution of investigations by all 50 states attorneys general where Blackbaud paid $49 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.'" (A0084-85 (¶¶87-88 n.16)) (quoting Delaware Attorney General press release). The attorneys' general investigations and settlements confirmed that Blackbaud housed confidential information of consumers, including HIPAA-protected information. (A0084-87 (¶¶87-91)).

The Complaint alleges that Blackbaud knew that social security and bank account information was exfiltrated as of July 21, 2020, several weeks before its August 4, 2020 10-Q was filed and two months before its 8-K was filed. (A0083-84 (¶¶79-84)). The Complaint further alleges that the SEC and all 50 states attorneys general investigated Blackbaud for the misstatements contained in its 8-K about the Data Breach and leveled combined penalties of $52 million against Blackbaud as a result. (A0084-87 (¶¶85-91)).

E. THE INSUREDS' INVESTIGATIONS & RESULTING EXPENSES

Instead of completing a full investigation and notifying the Insureds about the nature and scope of the data that was exfiltrated in the Data Breach, Blackbaud passed the buck to the Insureds by providing them with a "Toolkit" that instructed them to conduct their own independent investigations. (A0102-05 (¶¶139-156)). In addition to making misstatements about the Data Breach, the Toolkit also instructed

the Insureds to "look at the data fields you use in your Blackbaud Solution that was involved in this incident"—in other words, the very information under Blackbaud's custody and care. (A0104-05 (¶150)). The Toolkit provided the Insureds with a laundry list of to-do items such as consulting with legal counsel and notifying donors. (A0102-03 (¶144)). As a first step, the Insureds were required 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." (A0251-52) (emphasis in original).

The Insureds' investigations were 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 was exfiltrated too. (A0113 (¶185)). 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. (A0088 (¶95)). 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 notification requirements, and the costs of notification to their donors, accordingly. (*See* A0088-89, A0095-96, A0098-101, A0105 (¶¶99-100, 121-26, 132-37, 152-56)). Those damages amount to more than $1.5 million. (A0101 (¶¶135-37)).

F. STAGE OF THE PROCEEDINGS

Travelers filed its initial complaint on December 13, 2022. (A0020-33). On January 5, 2023, Blackbaud filed an answer to the original complaint, followed by an amended answer on January 26, 2023. On February 13, 2023, Blackbaud filed a Motion to Dismiss and Motion for Judgment on the Pleadings. Oral argument was held on January 6, 2024. The Superior Court granted Blackbaud's Motion to Dismiss on March 27, 2024. (A0034-66). Travelers filed a Motion for Reargument, which was denied on April 19, 2024, but allowed Travelers to amend.

On May 17, 2024, Travelers filed the operative Complaint and Jury Demand. (A0067-216). On June 28, 2024, Blackbaud filed a Motion to Dismiss the Complaint. Oral argument was held on December 13, 2024. (A0262-403). The Superior Court requested supplemental briefing, which was completed by the parties on January 10, 2025, and the court issued its Opinion and Order dismissing the Complaint with prejudice on April 3, 2025. (Ex. A).

Travelers filed its Notice of Appeal on May 2, 2025. (A0418-20).

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 Travelers failed to state a claim for breach of contract under the minimal notice pleading requirements of Superior Court Civil Rules 8 and 12(b)(6). (Preserved at A0231-37, A0315, A0318-19, A0324-25, A0331-32).

B. Scope of Review and Legal Standard

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, we (1) accept all well pleaded factual allegations as true, (2) accept even vague allegations as "well pleaded" if they give the opposing party notice of the claim, (3) draw all reasonable inferences in favor of the non-moving party, and (4) do not affirm a dismissal unless the plaintiff would not be entitled to recover under any reasonably conceivable set of circumstances." *Cent. Mortg. Co. v. Morgan Stanley Mortg. Cap. Hldgs. LLC*, 27 A.3d 531, 535 (Del. 2011) (citation omitted).

This Court has 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.

To plead a claim under Superior Court Civil Rule 8(a), a plaintiff must 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." "Dismissal is appropriate only if 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 (citation omitted). "[T]o avoid dismissal under Delaware's notice pleading standard, a party 'need not plead evidence,' but at a minimum, must 'allege facts that, if true, state a claim upon which relief can be granted.'"[2] *Wellgistics, LLC v. Welgo, Inc.*, 2024 WL 4327343, at *7 (Del. Super. Sept. 27, 2024) (quoting *VLIW Tech., LLC v. Hewlett-Packard Co.*, 840 A.2d 606, 611 (Del. 2003)).

C. Merits of Argument

The Superior Court correctly observed that, under New York law (which governs the terms of the Contracts), "[t]o state a claim for breach of contract, a

[2] As the court correctly observed: "Because the Contracts provide that they are governed by New York law, the Court will apply New York substantive law. Delaware procedural law applies." (Op. at 18) (citation omitted).

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).

1. The Complaint Adequately Alleges the Existence of a Contract

As to the first element, the Superior Court stated 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) (citing A0071-72 (¶¶18-20)). "Blackbaud was contractually required to safeguard 'Confidential Information' (defined to include: '(iii) donor, student, prospect and financial information') using "'commercially reasonable' cybersecurity procedures." (*Id*.) (quoting A0192 §6.a.). "Specifically, Section 6 of the Contracts 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). In the event of a data breach, Blackbaud contractually committed to notify the Insureds within 72 hours and had a ***separate*** obligation to "'use commercially reasonable efforts to mitigate any negative consequences resulting directly from the [Data Breach] ….'" (Op. at 4-5) (citing A0192 §6.c.).

2. The Complaint Adequately Alleges Breach of the Contract

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) (citing A0085, A0091-92, A0107-08, A0110-12 (¶¶88, 111, 164-68, 175-77)). The court acknowledged that the Contracts were the same for all the Insureds. (Op. at 1). The court further expounded:

> 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) (emphasis added; citations omitted).

Earlier, the court described Plaintiffs' well-pled allegations of "**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 A0076-78, A0078-79 (¶¶35-46, 52-56)).

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 [Contracts]." (A0091 (¶108); *see also* A0108, A0110-12 (¶¶167.d., 177)). This allegation was supported by the Delaware Attorney General's own conclusions alleged in the regulatory settlement with Blackbaud, quoted by the 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 A0084-85 (¶87)) (emphasis added).

The Complaint further alleges that Blackbaud knew that social security and bank account information was exfiltrated as of July 21, 2020, several weeks before its August 4, 2020 10-Q was filed and two months before its 8-K was filed. (A0083-84 (¶¶79-84)). Moreover, the SEC and all 50 states attorneys general investigated Blackbaud for the misstatements contained in its 8-K about the Data Breach and leveled a combined $52 million in penalties against Blackbaud as a result. (A0084-86 (¶¶85-91)).

The foregoing allegations are sufficient to state a claim for breach of contract.

Notwithstanding these allegations, the court below stated in a footnote that the Complaint "contain[s] 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." (Op. 15 n.58). Applying an erroneous heightened pleading standard to Travelers—one that may apply under Court of Chancery Rule 23.1, but does not apply to this Superior Court action—the court reasoned, "[r]ather, 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[,]" and finding that any "attempt to assert that the July disclosure was intentionally misleading, … has no factual support." (*Id.*). Travelers was entitled to have all inferences regarding Blackbaud's knowledge and intent drawn in Travelers' favor under Rule 8(a), and the Superior Court's holding to the contrary was error.

3. The Complaint Adequately Alleges Damages Suffered from the Breach of Contract

As to damages, the Superior Court summarized the Complaint's allegations that "[t]he Insureds incurred expenses to investigate and comply with their obligations under applicable laws." (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.
>
> 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. 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.

(*Id.* at 13-14) (citing A0098-101 (¶¶133-37)).

The Superior Court recognized that the Insureds allege that they undertook these investigative steps and incurred the expenses in direct response to Blackbaud's own instructions in the form of a "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) (citing A0102-04 (¶¶140-46)). As the 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, 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 A0102-03 (¶¶142, 144)). (*See also* Op. at 26 ("[E]ach [Insured] was forced to conduct its own investigation, as the Toolkit suggested.")). Thus, the Insured incurred these damages regardless of the types of data they were storing on Blackbaud's systems.

4. The Allegations of Breach Are Not Conclusory and Are Adequately Pled for Each Insured

Based on the foregoing, the Superior Court's own recitation of the alleged facts establishes the existence of a contract, breach of that contract, and damages resulting from that breach—in other words, a *prima facie* claim for breach of contract that satisfies the requirements of Rules 8 and 12(b)(6). Under Delaware's notice pleading standard, "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) (citation omitted). "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*, 2024 WL 4327343, at *7 (quoting *VLIW Tech*, 840 A.2d at 611). As the Superior Court further acknowledged, to adequately plead a breach of contract claim, "[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 may be pled generally[,]" but a party 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) (emphasis added) (citations omitted). Dismissal is appropriate only where "'it appears with reasonable certainty that the plaintiff could not prove any set of facts that would entitle him to relief[;]'" and "[a]n 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 (citations omitted). "[T]he trial court ***must*** draw all reasonable factual inferences in favor of the party opposing the motion." *Id.* (emphasis added).

The court itself appeared to recognize the veracity and simplicity of this very point during the argument on Blackbaud's motion to dismiss, stating: "they've [Plaintiffs] stated a general -- they 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." (A0379-80).

Despite this clarity in the court's understanding and recitation of Travelers' allegations and the terms of the Contracts, the court reached the wrong conclusion in its Opinion, erroneously finding that Travelers failed to state a claim for breach of contract under Delaware's liberal pleading standards. (Op. at 3). The question is how this plot twist came about.

It appears that the court failed to draw all reasonable factual inferences in Travelers' favor, as it must, in two ways: (1) by erroneously concluding that the Complaint impermissibly "aggregated" the Insured's claims together instead of providing separate allegations for each, and (2) relatedly, by erroneously concluding that the Complaint's allegations are "conclusory" rather than well-pled. (*Id.* at 2-3). Both conclusions are wrong and hold Travelers to a higher pleading standard than is 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 of the existence of a contract, breach of that contract, and damages resulting from that breach—for ***each*** Insured—that are sufficient to place Blackbaud on notice of the claims asserted against it and Travelers' theory of damages.

a. The Complaint Adequately Alleges Damages to Each Insured

Turning to the specifics of the court's reasons for concluding that the Complaint failed to state a claim for breach of contract, the court below first held (without citing any authority) that: "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." (Op. at 21) (emphasis in original).

In fact, Travelers pled just that. It alleged that each of its clients entered into the same Contract with Blackbaud. (A0071-72 (¶19)). It pled specific facts surrounding the alleged breach—the Data Breach—and the provisions of the Contracts that were breached—Sections 6.a.-d. (A0076-82, A0089-94 (¶¶36-72, 101-15)). Those facts were the same for all of the Insureds. (*See* Op. at 1). Finally, Travelers alleged that the damages incurred by the Insureds flowed from the Data Breach and Blackbaud's breach of the Contracts. (A0095-101 (¶¶121-37)). Despite this, the court's specific concern was that the Complaint lacked specifics about what data each Insured had stored with Blackbaud and what privacy law requirements any Insured was required to satisfy. (*See* Op. at 21-22) (citing A0098-101 (¶¶132-34)).

During oral argument on the motion to dismiss, however, the court recognized, correctly, that these details would ***not*** matter because the Complaint alleges that Blackbaud's security measures breached the Contracts by not being commercially

reasonable, and as a result of that breach, the Insureds would be required to conduct their own investigations due to the Data Breach regardless of what data they had stored and which privacy laws they had to satisfy:

> THE COURT: … [W]hether the toolkit was sufficient or not, 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 [sic]?

(A0375 (emphasis added); *see also* A0279-80, A0337-78).

The Superior Court additionally concluded that the Complaint failed to state a claim because it did "not include Insured-specific factual allegations of the type(s) of Expenses allegedly incurred." (Op. at 22). But the court never explained why this level of detail was necessary under Delaware's notice pleading standard.

The Complaint alleges that: "Under applicable data privacy laws and regulations, the 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")." (A0088 (¶97)). It further alleges that: "Plaintiff 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 [Contract] …." (A0089 (¶100)). 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. retain outside counsel to identify, assess, and comply with the legal obligations triggered by the Incident under laws and regulations;
>
> b. retain 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. retain outside counsel and print vendors to draft, translate, print, and mail letters under laws and regulations, or to undertake such work themselves;
>
> d. retain vendors to respond to third-party inquiries, such as regulators and Consumers; and/or
>
> e. incur other expenses as required under laws and regulations.

(A0100-01 (¶134); *see also* A0098-100, A0116-17 (¶¶133, 192)).

As the court itself also recognized, "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." (Op. at 14). Thus, fairly read and with all reasonable inferences being drawn in Travelers' favor, the Complaint alleges the identities of ***each*** Insured,

the types of expenses incurred as a result of Blackbaud's breach of the Contracts, and the total amount of expenses incurred by ***each*** Insured. These allegations are sufficient to provide general notice to Blackbaud of the claims asserted against it, and there is simply no need for further detail at the pleading stage under the liberal notice pleading requirements. *See Lawyers' Fund for Protection of Sate of New York v. JP Morgan Chase Bank, N.A.*, 915 N.Y.S.2d 741, 743 (N.Y. 2011) (finding allegations sufficient to defeat a motion to dismiss that set forth the "number of complaints, time frame within which their losses occurred, and the aggregate amount of damages").

"Additionally, whether damages are direct or consequential is a fact question, which cannot be decided at [the motion to dismiss] stage of the litigation." (Op. at 17). *See WSFS Fin. Corp. v. Great Am. Insur. Co.*, 2019 WL 2323839, at *7 (Del. Super. May 31, 2019) (holding that "whether the costs were foreseeable is a fact-based inquiry, which the Court should not resolve at the motion to dismiss stage") (citing *Frank Invests. Ranson, LLC v. Ranson Gateway, LLC*, 2016 WL 769996, at *13 (Del. Ch. Feb. 26, 2016)). A determination of whether all of the alleged expenses are recoverable is a matter for discovery and may potentially be addressed through summary judgment. *Klein v. Sunbeam Corp.*, 94 A.2d 385, 391 (Del. 1952) ("The present rules adopt a system of notice pleading rather than fully informative pleading as was theretofore required. The theory underlying the present rules is that

a plaintiff must put a defendant on fair notice in a general way of the cause of action asserted, which shifts to the defendant the burden to determine the details of the cause of action by way of discovery for the purpose of raising legal defenses."); *In re Asbestos Litig.*, 1994 WL 721774, at *2 (Del. Super. Nov. 4, 1994) ("It must be kept in mind that under our 'notice pleading' system, Rule 56 is the principal means by which factually unsupported claims or defenses are disposed and serves to conserve public and private resources.").

There is no support for the Superior Court's imposition of a higher pleading standard requiring Travelers to plead Insured-by-Insured claims with detailed factual particularity beyond the Delaware notice pleading standard. (Op. at 22-25). The Superior Court relied on three New York cases cited by Blackbaud for the proposition that Travelers had failed to adequate plead a claim, quoting: "'At 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.*'" (*Id.* 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. 2003)) (emphasis in original); *see id.* at n.79 (quoting *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 v. Philip Morris USA Inc.*, 729 N.Y.S.2d 240 (N.Y. 2000)). Nothing in those cases, however, requires 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* case, 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*, 729 N.Y.S.2d 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. *Lawyers' Fund* held "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.*

Finally, the Superior Court's conclusion that additional information about each Insured's claim—including the precise type of information that each ***stored on Blackbaud's systems***—was necessary to permit Blackbaud to defend itself was self-evidently erroneous. (Op. at 21). Travelers specifically alleged and argued that Blackbaud has ready access to the Insureds' accounts, and that the types of data that were housed in Blackbaud's systems could be investigated upon notice and identification of the affected Insureds. (A0073 (¶24), A0257, A0333). The court misconstrued this as an attempt by Travelers to argue bad faith by Blackbaud and found that facts supporting Blackbaud's acceess missing from the Complaint. (A0333-34). Neither of these conclusions is correct, as Travelers raised the fact of Blackbaud's access to demonstrate that the specific allegations in the Complaint coupled with Blackbaud's own internal information about the scope of the Data Breach are sufficient to place Blackbaud on notice of the claims against it. (*See* A0332-34).

b. The Complaint Adequately Alleges Proximate Cause

The Superior Court also found that the Complaint failed to allege proximate cause linking the Expenses (i.e., damages) to the Contracts. (Op. at 28-29). In so holding, the court appears to have conflated two separate contractual obligations on

the part of Blackbaud. Specifically, and without citation to the record, the court 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). Not so. Blackbaud's mitigation obligations appear in ***Section 6.d.*** of the Contracts. (*Id.* at 5). These are ***separate*** obligations from Blackbaud's promise under ***Section. 6.a.*** to "maintain commercially reasonable information security procedures and standards." (A0192). 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 alleges. (A0091, A0107-08, A0110-12 (¶¶108, 167.d., 177)). And as further set forth above, the Complaint alleges damages flowing from Blackbaud's failure to maintain commercially reasonable information security procedures and standards. (A0088, A0089, A0100-01, A0116-17 (¶¶97, 100, 134, 192)).[3]

[3] To be clear, Travelers does also allege that Blackbaud breached its mitigation obligations. But that separate alleged breach is unnecessary for Travelers to plead that Blackbaud's failure to maintain commercially reasonable information security procedures and standards resulted in damage. (*See* A0287-88: "THE COURT: Here, ***one of the promises Blackbaud made*** was to use commercially reasonable measures to prevent the hack. … So why don't these damages that they're alleging flow from that?") (emphasis added). It is unnecessary for this Court to opine on the adequacy of Travelers' 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.

The Superior Court also suggested that Travelers was attempting "to essentially impose strict liability on Blackbaud for every data breach where the parties expressly agreed to a risk allocation scheme," i.e., the liability limitations in Section 10 of the Contracts. (Op. at 28). That is incorrect. Travelers only seeks to hold Blackbaud liable for Data Breach resulting from Blackbaud's contractual breaches—including the breach of its obligations under Section 6.a. of the Contracts to maintain commercially reasonable security procedures and standards. By finding that the liability limitation provision vitiated causation even when the damages resulted from an actual breach, the Superior Court effectively and improperly read Blackbaud's obligations under Section 6.a. out of the Contracts. *God's Battalion of Prayer Pentecostal Church, Inc. v. Miele Associates, LLP*, 845 N.E.2d 1265, 1267 (N.Y. 2006) ("A contract 'should be read to give effect to all its provisions.'") (citations omitted).

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 Complaint with prejudice. (Preserved at A0224, A0257, A0414).

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 (Table) (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, to the extent that the Superior Court properly dismissed the Complaint for failure to state a claim, the dismissal should have been without prejudice, as Travelers requested in response to the motion to dismiss. (A0224, A0257). As recited by the court, "[d]ismissal will be denied if there is a reasonably conceivable set of circumstances of recovery on the claim," and "the court should dismiss a claim 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.'" (Op. at 18) (citations omitted).

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 *2 (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."). "Justice may not so require if the party seeking to amend has been inexcusably careless or if the amendment would unfairly prejudice an opposing party." *Annone v. Kawasaki Motor Corp.*, 316 A.2d 209, 211 (Del. 1974). The court below did not engage in any analysis before erroneously holding that, "[b]ecause this was Plaintiffs' second attempt to adequately plead their claims, the amended complaints are ***dismissed with prejudice***." (Op. at 27) (emphasis in original).

Putting aside whether the Complaint's allegations adequately satisfy the applicable pleading standards, the court did not find that Travelers 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. (*See* Op. at 2-3, 33). 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." (*Id.* at 27). At the very least, Travelers should be given the opportunity

to amend its Complaint to provide the information that the court says is missing, as it requested in its Answering and Supplemental Briefs. (A0224, A0257, A0414).

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.

CONCLUSION

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

HEYMAN ENERIO
GATTUSO & HIRZEL LLP

/s/ Kurt M. Heyman
Kurt M. Heyman (# 3054)
Gillian L. Andrews (# 5719)
222 Delaware Avenue, Suite 900
Wilmington, DE 19801
(302) 472-7300
Attorneys for Plaintiff-Below and Appellant Travelers Casualty and Surety Company of America

Dated: June 12, 2025

CERTIFICATE OF SERVICE

Kurt M. Heyman, Esquire, hereby certifies that on June 12, 2025, copies of the foregoing Opening Brief of Appellant Travelers Casualty and Surety Company of America were served electronically on the following:

John P. DiTomo, Esquire
Elise Wolpert, Esquire
Morris, Nichols, Arsht
& Tunnell LLP
1201 North Market Street
Wilmington, DE 19801

Emily C. Friedman, Esquire
Ballard Spahr LLP
919 North Market Street, 11th Floor
Wilmington, DE 19801

Wade A. Adams, III, Esquire
The Law Offices of Wade A. Adams III
111 Continental Drive, Suite 309
Newark, DE 19713

Kenneth T. Levine, Esquire
De Luca Levine LLC
301 E Germantown Pike 3rd Floor,
East Norriton, PA 19401

/s/ Kurt M. Heyman
Kurt M. Heyman (# 3054)