IN THE SUPREME COURT OF THE STATE OF DELAWARE

TRAVELERS CASUALTY AND SURETY COMPANY OF AMERICA, and PHILADELPHIA INDEMNITY INSURANCE COMPANY, ACADIA INSURANCE COMPANY, and UNION INSURANCE COMPANY,	§	C.A. No. 193, 2025 C.A. No. 198, 2025 Court Below: Superior Court of the State of Delaware
Plaintiffs Below, Appellants,	§	C.A. No. N22C-12-130 C.A. No. N22C-12-141
v.	§	
BLACKBAUD, INC.,	§	
Defendant Below, Appellee.	§	

Submitted: November 19, 2025
Decided: February 13, 2026

Before **SEITZ**, Chief Justice; **VALIHURA**, **TRAYNOR**, **LEGROW**, and **GRIFFITHS**, Justices, constituting the Court *en Banc*.

Upon appeal from the Superior Court. **REVERSED AND REMANDED**.

Kurt M. Heyman, Esquire, (*argued*), Gillian L. Andrews, Esquire, HEYMAN ENERIO GATTUSO & HIRZEL LLP, Wilmington, Delaware, *for Travelers Casualty and Surety Company of America, Plaintiff Below/Appellant*.

Lisa C. McLaughlin, Esquire, PHILLIPS, McLAUGHLIN & HALL, P.A., Wilmington, Delaware; Kenneth T. Levine, Esquire, (*argued*), de LUCA LEVINE LLC, East Norriton, Pennsylvania, *for Philadelphia Indemnity Insurance Company, Acadia Insurance Company, and Union Insurance Company, Plaintiffs Below/Appellants*.

John P. DiTomo, Esquire, Jialu Zou, Esquire, MORRIS, NICHOLS, ARSHT & TUNNELL LLP, Wilmington, Delaware; Sarah Fulton Hutchins, Esquire, (*argued*), Corri A. Hopkins, Esquire, PARKER POE ADAMS & BERNSTEIN LLP, Charlotte, North Carolina, *for Blackbaud, Inc., Defendant Below/Appellee*.

SEITZ, Chief Justice:

Blackbaud, Inc., a software application and data hosting provider for non-profits, suffered a major ransomware attack. The hacker infiltrated Blackbaud's servers and stole sensitive client data. Blackbaud's clients lost faith that the company would address the harm and reimburse them for their losses. The clients conducted their own investigations and took remedial steps to mitigate their losses. Their insurers covered some of the losses and then sued Blackbaud as subrogees/assignees to recover their payments to the insureds.

The Superior Court dismissed the original complaints for failing to state a claim. In response, the insurers filed amended complaints. The Superior Court dismissed the amended complaints, this time with prejudice. It held that the insurers failed to allege factual support for each Blackbaud client's claims and, as a legal matter, failed to plead proximate cause.

On appeal, the insurers argue that the court should not have dismissed the amended complaints because they met the Superior Court's minimum pleading requirements. They also contend that the court should not have dismissed the amended complaints with prejudice. For the reasons explained below, we reverse because the insurance carriers, as subrogees/assignees, adequately pled a breach of contract claim in their amended complaints. Given our ruling, we need not address the second issue on appeal.

I.

A.

According to the amended complaints, Blackbaud is a software company that provides donor relationship management software and information technology services to their educational and non-profit clients.[1] Travelers Casualty and Surety Company of America ("Travelers"), Philadelphia Indemnity Insurance Company, Acadia Insurance Company, and Union Insurance Company ("Philadelphia Indemnity") (together with Travelers the "Insurers") provided insurance coverage to 97 of Blackbaud's educational and non-profit clients for cyber and criminal incidents like data breaches.[2]

The Insurers wrote policies that covered losses in excess of retentions for damages caused by data breaches.[3] The policies allowed the Insurers to subrogate, or stand in the shoes of the insureds, to recoup payments for certain losses arising from data breaches.[4] The Insurers also obtained contract assignments from Blackbaud clients.[5] We will refer to the Blackbaud clients as the "Insureds."

---

[1] App. to Philadelphia Opening Br. at A66-67 [hereinafter A___]; App. to Travelers Opening Br. at AA70-71 [hereinafter AA___].

[2] A63-65, A67; AA69-71, AA189.

[3] A62, A65-66; AA68-70.

[4] A65-66; AA70.

[5] A180; AA195.

B.

Blackbaud and the Insureds signed Blackbaud Solutions Agreements (the "Agreements").[6] The Agreements were identical for all the Insureds and are governed by New York law.[7] Blackbaud hosted the Insureds' sensitive donor data on its servers.[8] The Insureds used Blackbaud's software applications to collect payments and transact with donors.[9] In the Agreements, Blackbaud agreed to protect the Insureds' sensitive data as follows:

- maintain administrative, physical, and technical safeguards;
- protect against anticipated threats or hazards to the security of confidential information;
- protect against unauthorized access to or use of confidential information that could materially harm the Insureds;
- maintain commercially reasonable information security procedures and standards;
- implement commercially reasonable, written policies and procedures addressing potential security breaches;
- have a breach response plan in place; and

[6] A67, A176-180; AA71-72, AA191-95.

[7] A176-180; AA191-95.

[8] A67-69, A71; AA71-73, AA76.

[9] A67; AA71.

- use commercially reasonable efforts to mitigate any negative consequences resulting directly from a breach and provide 72-hour notice of any breach.[10]

C.

In 2020, a cyber attacker accessed Blackbaud's system for several months and exfiltrated confidential customer data from its servers.[11] The attacker threatened to publish the data unless Blackbaud paid a ransom.[12] On July 16, 2020, Blackbaud revealed the breach on its website.[13] The website notice stated that "**[n]o action is required on your end because no personal information about your constituents was accessed**."[14]

Blackbaud filed a Form 10-Q on August 4, 2020, disclosing the breach but characterizing the exfiltration of sensitive donor information as hypothetical.[15] In a later September 29, 2020 Form 8-K filing, Blackbaud stated that "the cybercriminal may have accessed some unencrypted fields intended for bank account information,

---

[10] A177; AA192.

[11] A72-76; AA78-80.

[12] A75; AA80. This data included full names, age, date of birth, social security numbers, home addresses, phone numbers, email addresses, financial information, medical information, gender, religious beliefs, marital status, spouse names, spouses' donation history, employment information, educational information, and account credentials. A75; AA81.

[13] A76; AA82-83.

[14] A76; AA83 (emphasis in original).

[15] A77; AA83.

social security numbers, usernames and/or passwords."[16]

In 2023, Blackbaud agreed to pay a $3 million fine to the Securities and Exchange Commission to resolve charges that the company made misleading disclosures about the cyber security attacks.[17] Blackbaud also paid $49 million to resolve state law claims brought by the attorneys general of all 50 states.[18]

D.

The Insureds claimed that, instead of addressing the cyberattack and protecting the Insureds, Blackbaud failed to conduct an adequate investigation of the breach.[19] They also contended that, even though sensitive customer data resided on Blackbaud's servers, Blackbaud shifted the investigative burden and remediation efforts onto the Insureds.[20] For instance, Blackbaud provided the Insureds a "Toolkit" with instructions to complete their own investigations.[21] The Toolkit listed "next steps," such as investigating the data involved in the breach, consulting with legal counsel, and notifying compromised donors.[22]

---

[16] A77; AA84.

[17] A78; AA84.

[18] A78-80; AA84-87.

[19] A91-94; AA98-101.

[20] A94-98; AA101-105.

[21] A94-96, A181-91; AA102-05, AA196-206.

[22] *Id.*

Dissatisfied with Blackbaud's response to the cyberattack, the Insureds conducted their own investigations and remediation and made claims against their insurance policies for those expenses.[23] Philadelphia Indemnity paid over $600,000 to its Insureds.[24] Travelers paid over $1.5 million.[25]

E.

The Insurers filed suit against Blackbaud in Superior Court as subrogees/assignees of their Insureds. They alleged breach of contract and negligence claims against Blackbaud and sought to recover payments the Insurers made to their Insureds for investigation and remediation expenses.[26] Blackbaud responded with a motion to dismiss and for judgment on the pleadings. The court granted Blackbaud's motion. It held that the original complaints failed to state a claim for breach of contract, negligence, or gross negligence.[27]

After the court denied their motion for reargument, the Insurers filed amended complaints.[28] The court dismissed the amended complaints, this time with

---

[23] A91-94; AA95-101.

[24] A62, A94.

[25] AA68, AA101.

[26] A14-27; AA20-33.

[27] *Travelers Cas. & Surety Co. of Am. v. Blackbaud, Inc.*, 2024 WL 1298762, at *13 (Del. Super. Mar. 27, 2024).

[28] A61-111; AA67-124.

prejudice.[29] It found that "a complaint must include specific allegations supported by facts," and by pleading the Insureds' claims in the aggregate, the Insurers "fail[ed] to provide the required factual support for any insured's claim and d[id] not adequately allege a subrogation claim."[30] The court also held that, even if pleading in the aggregate was sufficient, "the amended complaints fail to adequately plead proximate cause because they fail to link the alleged damages to any contract term."[31] To plead proximate cause, the court held, the Insurers could not rely on a contract term "that required Blackbaud to mitigate negative consequences of a data breach."[32] Finally, the court held that the Insureds could not rely on "conclusory allegations of misrepresentations" to plead proximate cause.[33]

II.

On appeal, the Insurers argue that the Superior Court erred when it found that the Insurers could not, as a matter of law, plead their breach of contract claims in the aggregate. According to the Insurers, nothing in Delaware law prohibits aggregated pleading of subrogation claims, and any other rule would be contrary to Superior

---

[29] *Travelers Cas. & Surety Co. of Am. v. Blackbaud, Inc.*, 2025 WL 1009551, at *15 (Del. Super. Apr. 3, 2025) [hereinafter *Travelers II*].

[30] *Id.* at *1.

[31] *Id.*

[32] *Id.*

[33] *Id.* at *2.

Court Civil Rule 8(a)'s notice pleading requirements. And second, they argue that, at the motion to dismiss stage, they were not required to link the alleged damages to any specific contract term. We review *de novo* the court's decision to dismiss for failure to state a claim.[34]

A.

Blackbaud does not dispute that the Insurers stand in the shoes of the Insureds and, as subrogees/assignees, have standing to pursue their Insureds' breach of contract claims against Blackbaud. Blackbaud also does not contest that the contracts are governed by the substantive law of New York and that the pleading requirements are governed by Delaware law – specifically, Superior Court Civil Rule 8(a). Thus, the issue before us *de novo* is whether the Insurers have met Rule 8(a)'s pleading requirements for a breach of contract action governed by New York law.

Under New York law, a breach of contract claim has four elements: "the existence of a contract, the plaintiff's performance under the contract, the defendant's breach, and resulting damages."[35] Under Superior Court Civil Rule 8(a), the plaintiff must provide "(1) a short and plain statement of the claim showing that

---

[34] *Thompson St. Cap. Partners IV, L.P. v. Sonova U.S. Hearing Instruments, LLC*, 340 A.3d 1151, 1164-65 (Del. 2025); *City of Fort Myers Gen. Emps.' Pension Fund v. Haley*, 235 A.3d 702, 716 (Del. 2020). The Insurers have not appealed dismissal of their negligence claims.

[35] *Detringo v. S. Island Fam. Med., LLC*, 71 N.Y.S.3d 525, 527 (N.Y. App. Div. 2018) (citations omitted).

the pleader is entitled to relief and (2) a demand for judgment for the relief to which the party deems itself entitled."

In *Central Mortgage Company v. Morgan Stanley Mortgage Capital Holdings LLC*, we held that:

> [A] court should accept all well-pleaded factual allegations in the Complaint as true, accept even vague allegations in the Complaint as "well-pleaded" if they provide the defendant notice of the claim, draw all reasonable inferences in favor of the plaintiff, and deny the motion unless the plaintiff could not recover under any reasonably conceivable set of circumstances susceptible of proof.[36]

Here, the Insurers—standing in the shoes of the Insureds—met the Superior Court's pleading requirements to state a breach of contract claim under New York law. First, the Insurers alleged "the existence of a contract." According to the Superior Court, "[e]ach Insured entered into a separate 'Solutions Agreement' with Blackbaud[.]"[37] Second, the Insurers alleged the Insureds performed under the contract.[38] Third, the Insurers alleged that "the contract was breached." As set forth in detail above, the Insurers identified each of Blackbaud's contractual duties specific to sensitive data management and data breach response, and how Blackbaud

---

[36] 27 A.3d 531, 536 (Del. 2011). In *Central Mortgage*, we decided not to follow the federal court pleading standards. *Id*. at 537.

[37] *Travelers II*, 2025 WL 1009551, at *2.

[38] A110 ("The Insureds have complied with any and all conditions precedent to recovery under their agreements with Blackbaud."); AA123 (same).

breached those contractual provisions. In the words of the Superior Court:

> 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.[39]

[39] *Travelers II*, 2025 WL 1009551, at *5-6 (citations omitted).

And fourth, the Insurers alleged "damages [the Insureds] suffered as a result of the breach." Again, in the words of the Superior Court:

> 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.[40]

Even though the Insurers touched each base for a breach of contract claim under New York law, the Superior Court dismissed their claims. According to the court, the Insurers came up short on two grounds—the Insurers could not, as a pleading matter, aggregate the Insureds' claims in a subrogation complaint, and the Insurers failed to plead proximate cause. We address each ground in turn.

---

[40] *Id.* at *6-7 (citations omitted).

B.

The Superior Court held that the amended complaints did not state a subrogation claim under Superior Court Civil Rule 12(b)(6). According to the court, by pleading the Insureds' claims in the aggregate, the Insurers failed to provide the required factual support for each Insured's claim. Specifically, the court held that the Insurers were required to plead data breach-related information specific to each Insured, specify the privacy law requirements each Insured had to satisfy, and list the types of expenses each Insured allegedly incurred responding to the breach. Otherwise, the court held, Blackbaud could not defend against the claims.

We are not persuaded that Blackbaud was at a disadvantage in defending against the allegations of the amended complaints. Blackbaud controlled its information technology systems and knew what sensitive information was accessed. After discovery aimed at each Insured, Blackbaud can amend its answer and assert new defenses specific to each Insured.[41] And if the Insurers claimed damages for losses that are capped by, or not covered by, the Agreements, Blackbaud could move for summary judgment on those losses.

The court recognized that no Delaware precedent required pleading individualized claims in subrogation actions.[42] Nonetheless, it turned to a few New

[41] Super. Ct. Civ. R. 15.

[42] *Travelers II*, 2025 WL 1009551, at *9.

York decisions addressing equitable subrogation pleading requirements when healthcare providers attempt to recover their cost of care in mass tort cases.[43] In those cases, the New York courts dismissed equitable subrogation claims because the healthcare entities failed to identify each harmed patient. And, according to the New York courts, the claims were so unique to the individuals harmed that the defendants could not be expected to address them in the aggregate.[44]

Here, however, the Insurers did not seek equitable subrogation to recover costs paid to an amorphous group of individuals with unique harms.[45] Instead, they

---

[43] *Id.* at *10 n.79; *Blue Cross & Blue Shield of N.J., Inc. v. Philip Morris USA Inc.,* 344 F.3d 211, 218 (2d Cir. 2003) (finding the insurer was required to identify the subrogors and their claims so defendants could assert defenses against those claims); *A.O. Fox Mem'l Hosp. v. Am. Tobacco Co., Inc.*, 754 N.Y.S.2d 368, 369 (N.Y. App. Div. 2003) (finding plaintiffs failed to identify individual patients and their specific injuries and specify facts to establish liability); *E. States Health & Welfare Fund v. Philip Morris, Inc.*, 729 N.Y.S.2d 240, 252 (N.Y. Sup. Ct. 2000) (finding defendants could not "fairly defend" against claims without knowing what the specific injuries were for each person).

[44] In *Lawyers' Fund For Client Prot. of State of N.Y. v. JP Morgan Chase Bank, N.A.*, 915 N.Y.S.2d 741, 743 (N.Y. App. Div. 2011), the court recognized that other New York decisions dismissed complaints with aggregated claims that "involved such a high degree of individualized inquiry" that failing to identify them would not establish a subrogation claim. But in *Lawyers' Fund*, the court affirmed the denial of a motion to dismiss notwithstanding aggregated damages because the subrogors were a small, clearly defined, and readily identifiable group who each sustained identical injuries from the same acts and omissions by a defendant with prior knowledge of the claimants.

[45] Equitable subrogation arises in equity and prevents unjust enrichment. It allows a party (like an insurer) who has paid a debt that should have been paid by another to "step into the shoes" of the creditor to recover that payment. Contractual subrogation, on the other hand, is grounded in a contract, typically an insurance contract, and the parties' relationship is governed by the contractual terms. *See Rodriguez v. Great Am. Ins. Co.*, 2022 WL 591762, at *7-8 (Del. Super. Feb. 23, 2022) (citing *E. Sav. Bank, FSB v. Cach, LLC*, 124 A.3d 585, 590 (Del. 2015)) (distinguishing equitable and contractual subrogation); *see also N.Y. Mun. Ins. Reciprocal v. Stewart's Shop Corp.*, 212 N.Y.S.3d 859, 860 (N.Y. App. Div. 2024) (same).

identified each of the Insureds,[46] the Blackbaud contract they had in common,[47] the shared bases for the breaches,[48] and the same or similar investigation and remediation damages incurred responding to the data breach.[49] Under *Central Mortgage*, nothing more was required to state a breach of contract claim under New York law. At bottom, Blackbaud objected to claim aggregation because it wanted more detail in the amended complaints about how each Insured responded to the data breach and the expenses they incurred. Those details were not needed to state a claim. They can be explored in discovery.

C.

Next, the Superior Court held that the Insurers failed to state a claim because they did not plead facts establishing proximate cause. The court confined the Insurers' proximate cause argument to two grounds—"Blackbaud's contractual promise to mitigate the impact of a data breach" and its "misrepresentations of the scope of the data breach."[50] As to the former, the court held that it would be unreasonable to interpret the mitigation provision to impose "strict liability" on

---

[46] A63-65; AA189.

[47] A176-180; AA191-95.

[48] A98-104; AA106-113.

[49] A104-110; AA113-123.

[50] *Travelers II*, 2025 WL 1009551, at *11, *13.

Blackbaud for every data breach.[51] As to the latter, the court held that there was no "reasonable reliance" term in the Agreements and the Insurers did not allege when the Insureds decided to conduct their own investigations.[52] Therefore, the court held, the proximate cause allegations were conclusory and should be dismissed.

Under New York law, the defendant's breach must be a "substantial factor in producing the damage."[53] Delaware and New York law are consistent that proximate cause is ordinarily determined by the trier of fact.[54] Here, the Insurers did not limit their causation arguments to one contractual provision or representation.[55] The Insurers pled that Blackbaud breached multiple information security promises in the Agreements and then shifted the investigation and remediation responsibilities onto

---

[51] *Id.* at *12.

[52] *Id.* at *14.

[53] *Fed. Hous. Fin. Agency v. Morgan Stanley ABS Cap. I Inc.*, 73 N.Y.S.3d 374, 397 (N.Y. Sup. Ct. 2018) (citations omitted).

[54] *Duphily v. Del. Elec. Co-op., Inc.*, 662 A.2d 821, 830 (Del. 1995) ("This Court has consistently held that the issue of proximate cause is ordinarily a question of fact to be determined by the trier of fact," a principle established in this Court's cases dating back to 1934.); *see also Voss v. Neth. Ins. Co.*, 22 N.Y.3d 728, 737 (N.Y. 2014) ("[Q]uestions of proximate cause and foreseeability should generally be resolved by the factfinder[.]").

[55] *See, e.g.,* A233-41; AA249-57 (Insurers argued that remediation expenses were proximately caused by Blackbaud's breaches of Sections 5(b), 6(a), and 6(b) of the Agreements, which included failing to protect the Insureds' confidential information and failing to have a response plan in place. Blackbaud also gave false assurances to the Insureds through its Toolkit, which was provided more than 72 hours after the data breach, in violation of Section 6(c).); A241; AA256 (The Insureds had no choice but "to fill the void and handle the fallout from Blackbaud's failures.").

the Insureds.[56] As a result of the data breach, the Insureds had to retain computer forensics firms to investigate and mitigate the breach; incur counsel fees to determine their responsibilities under federal and state law; notify customers; conduct credit monitoring and more. Once the plaintiff has alleged facts raising a reasonable inference that damages were caused by the defendant, damages may be pled generally.[57] After discovery, Blackbaud can attempt to limit its damages through applicable contractual damage limitations.

Under Delaware notice pleading standards, the amended complaints alleged facts from which—drawing all inferences in the Insurers' favor—a reasonable factfinder could find that Blackbaud's contractual breaches were the proximate cause of the Insureds' investigation and remedial expenses.

III.

The Insurers have stated a claim for breach of contract under New York law. The Superior Court's judgment is reversed and the case remanded for proceedings consistent with this opinion. Jurisdiction is not retained.

---

[56] A83-98; AA89-105.

[57] *Lebanon Cnty. Emp. Ret. Fund v. Collis*, 287 A.3d 1160, 1208 (Del. Ch. 2022) ("A court does not typically parse the scope of damages at the pleading stage. A plaintiff can plead the existence of damages generally as long as the complaint supports a reasonable inference of harm.") (citations omitted).