UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH CAROLINA
(COLUMBIA DIVISION)

IN RE: BLACKBAUD, INC., CUSTOMER DATA SECURITY BREACH LITIGATION	**Case No. 3:20-mn-02972-JFA** MDL No. 2972 **REDACTED PUBLIC FILING**

MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

MOTLEY RICE LLC

/s/ Marlon E. Kimpson
Marlon E. Kimpson (SC Bar No. 17042)
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Tel: (843) 216-9000
Fax: (843) 216-9027
Email: mkimpson@motleyrice.com

DiCELLO LEVITT LLC

/s/ Amy E. Keller
Amy E. Keller
Ten North Dearborn Street, 6th Floor
Chicago, IL 60602
Tel: (312) 214-7900
Email: akeller@dicellolevitt.com

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLP

/s/ Harper T. Segui
Harper T. Segui
825 Lowcountry Blvd., Suite 101
Mount Pleasant, SC 29464
Tel: (919) 600-5000
Fax: (919) 600-5035
Email: hsegui@milberg.com

SUSMAN GODFREY LLP

/s/ Krysta K. Pachman
Krysta K. Pachman
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
Email: kpachman@susmangodfrey.com

Interim Co-Lead Counsel for Plaintiffs

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Other Authorities

I. INTRODUCTION

Despite touting the safety of its data security platforms, Blackbaud's substandard data security practices are no secret on the dark web: hackers have been bragging about accessing and exfiltrating data from Blackbaud's systems for the past several years. And because Blackbaud has failed to adopt and implement the most basic (and necessary) cybersecurity defenses, it was vulnerable to attack—and was even unaware that its systems had been accessed and exploited until anonymous attackers demanded a ransom payment for a massive breach in 2020.

Between at least February 7 and May 20, 2020, [redacted] From that entry point, [redacted]. After finding it, the attackers copied and exfiltrated over [redacted] of data—including class members' unencrypted Social Security numbers, bank account and credit card information, and confidential medical information. The attackers planted notes in Blackbaud's systems announcing their "plains to publush" this stolen data and making ransom demands. Who "they" are remains unknown, along [redacted] were involved in the breach during this period. In response, and in disregard of the advice of law enforcement and security experts, Blackbaud paid [redacted] unknown attackers $230,000 for "proof" of destruction of the stolen data—[redacted]—but no [redacted] ever came.

The breach resulted from a litany of correctible, longstanding, cybersecurity deficiencies well known to Blackbaud. Blackbaud failed to close off a known vulnerability in its [redacted]—one so old that a Blackbaud security engineer lamented "what year is it?" after learning how the attackers exploited it to gain access to Blackbaud's systems. Beyond that, Blackbaud's outdated systems, [redacted]

[redacted] permitted the attackers to freely rove Blackbaud's systems for months, stealing class members' data, before Blackbaud even detected them.

Just as bad as Blackbaud's massive security lapses was its woefully inadequate and deceptive response to the breach. Blackbaud bragged that it "stopped" the breach, while neglecting to mention that it missed or mishandled alerts of the intrusion in February and March of 2020. On top of that, Blackbaud flatly told its customers and the public that the attackers "***did not access***" sensitive information like Social Security numbers and that it had received "***confirmation***" that the exfiltrated data had been destroyed. Both statements were false. It soon emerged that unencrypted Social Security numbers and bank account information had in fact been pervasively exposed in the breach. Since then, Blackbaud has maintained its evasive, "nothing to see here" approach, hiding information from regulators and keeping its customers, class members, and the public in the dark about the nature and severity of the breach. Its deliberate lack of transparency was so egregious that KPMG—one of Blackbaud's information security auditors—withdrew reports on its audit of Blackbaud for the 2018-19 period because it could no longer rely on representations made by Blackbaud's management about Blackbaud's response to the breach.

Blackbaud's failure to protect class members' personal data—and its compounding failures to investigate the breach and communicate truthfully about its scope and nature—has harmed Plaintiffs and members of the class. These harms are twofold. *First*, Blackbaud's inadequate data security measures and its response to the breach has put the victims of the data breach at severe risk of fraud, scams, identity theft, and social engineering. Personal information belonging to class members—including contact information, Social Security and passport numbers, financial account information, and medical treatment histories—is available to be sold and re-sold on the dark web, enabling those with access to the data to perpetrate myriad types of fraud on these individuals for

years to come. *Second*, these individuals' personal data has real, monetizable value, as demonstrated by [redacted], for the same people, that was compromised in the breach. As such, class members, who never consented to their data being disclosed to cybercriminals, have been harmed. To remedy these harms, Plaintiffs seek (i) the costs of insurance and monitoring necessary to protect these individuals against the risks described above and (ii) the lost value of their personal data. Additionally, several state laws provide for statutory damages without requiring proof of economic harm because it is recognized that such invasions of privacy require remedies not just to compensate injured persons, but to deter deficient practices that allow breaches to take place.

Blackbaud's wrongdoing and the harm to the members of the class present common issues of fact and law appropriate for class certification. Plaintiffs ask the Court to certify the following Classes and Sub-classes pursuant to Rule 23(b)(2) and 23(b)(3) to allow Plaintiffs to pursue remedies on behalf of all class members[1]:

i. Nationwide negligence and gross negligence classes under Massachusetts common law: All natural persons residing in the United States whose unencrypted information was stored on the database of a customer identified in Exhibit A to Defendant's Revised Fact Sheet from February 7, 2020 to May 20, 2020.

ii. California Consumer Privacy Act (CCPA) Sub-class: All natural persons residing in California whose unencrypted information (1) was stored on the database of a customer identified in Exhibit A to Defendant's Revised Fact Sheet from February 7, 2020 to May 20, 2020, and (2) contains the combination of data elements identified in Appendix 2 to this memorandum;

iii. California Confidentiality of Medical Information Act (CMIA) Sub-class: All natural persons residing in California whose unencrypted information (1) was stored on the database of a customer identified in Exhibit A to

[1] The Court's November 21, 2022 Order directed Plaintiffs to address their invasion of privacy claim in their class certification motion. ECF No. 285. Plaintiffs do not seek to certify a claim for invasion of privacy under Massachusetts law.

Defendant's Revised Fact Sheet from February 7, 2020 to May 20, 2020, and (2) contains the combination of data elements identified in Appendix 2 to this memorandum;

iv. New York General Business Law (NY GBL) Sub-class: All natural persons residing in New York (1) whose unencrypted information was stored on the database of a customer identified in Exhibit A to Defendant's Revised Fact Sheet from February 7, 2020 to May 20, 2020, and (2) who viewed or were exposed to Blackbaud's post-breach representations regarding the scope of the breach and the "confirmation" of destruction by the cybercriminals[2];

v. Florida Deceptive and Unfair Trade Practices Act (FDUTPA) Sub-class (seeking injunctive relief): All natural persons residing in Florida (1) whose unencrypted information was stored on the database of a customer identified in Exhibit A to Defendant's Revised Fact Sheet from February 7, 2020 to May 20, 2020 and (2) who viewed or were exposed to Blackbaud's post-breach representations regarding the scope of the breach and the "confirmation" of destruction by the cybercriminals.

II. BACKGROUND

A. Cybercriminals stole the personal information of millions of class members due to Blackbaud's inadequate data security.

By 2020, Blackbaud knew it was a prime candidate for a major data breach. In April 2019, Ricky Banda—a security engineer for Blackbaud—noted, [redacted] Ex. 2 (BLKB_MDL_00117549 at -117553). In June 2019, [redacted] Blackbaud's Senior Director of Risk and Compliance, listed the [redacted]

[2] Specifically, the representations that "The cybercriminal did not access credit card information, bank account information, or social security numbers"; and "Because protecting our customers' data is our top priority, we paid the cybercriminal's demand with confirmation that the copy they removed had been destroyed." *See* Ex. 1; Blackbaud, *Security Incident*, https://web.archive.org/web/20200719170537/https://www.blackbaud.com/securityincident (July 1, 2020 archive of website).

[redacted] Ex. 3 (BLKB_MDL_00056785). In November 2019, Rich Friedberg—Blackbaud's Chief Information Security Officer—painted a dire picture of the company's [redacted] Ex. 4 (BLKB_MDL_00117035 at -117036). He warned that the "current trajectory ***will take*** [redacted] ***. . . to achieve*** [redacted] ***in line with industry norms.***" *Id.* (emphasis added). For example, Blackbaud had "excessive technical debt . . . accumulated over decades"—technology and systems from other service providers that Blackbaud acquired with unknown or outdated systems that had yet to be fully integrated. *Id.* He also noted: [redacted][3] *Id.* at -117037. He cautioned that [redacted] Many of which not exercising appropriate care [redacted]." *Id.* As to [redacted], "[n]ot all areas of the infrastructure or applications [redacted] *Id.*

As if the numerous deficiencies known to Blackbaud's own Chief Information Security Officer weren't enough, in December 2019—just weeks before the data breach started—a firm

[3] [redacted]

specializing in cyberattack simulations warned Blackbaud that it was [redacted] Ex. 9 (BLKB_MDL_00055614 at -55616). It also noted [redacted] *Id.* And just days into the 2020 breach—which Blackbaud had not yet detected—Friedberg warned his boss, Chief Financial Officer Kevin McDearis, that [redacted] Ex. 10 (BLKB_MDL_00281501 at -281502).

But that's not all. Blackbaud had been passively tolerating other specific vulnerabilities for years. One related to [redacted] The feature could be [redacted] Ex. 11 (BLKB_MDL_00072686 at -72698). The potential for misuse of this feature has been known in the information security industry since May 2013. Ex. 12 (Nov. 5, 2021 Friedberg Tr.) at 212:5-213:12.[4] And Blackbaud, a company whose very existence was premised on securing confidential personal data, was specifically warned of

[4] *See also* Scott Sutherland, Breaking Out! of Applications Deployed via Terminal Services, Citrix, and Kiosks, Netspi (May 22, 2013), https://www.netspi.com/blog/technical/network-penetration-testing/breaking-out-of-applications-deployed-via-terminal-services-[redacted]-and-kiosks/ [https://perma.cc/9QB4-5Z7J].

this issue in 2016, when a cybersecurity firm called Praetorian issued a report to Blackbaud detailing this specific vulnerability in Blackbaud's systems and recommending that Blackbaud disable [redacted] to eliminate the vulnerability. Ex. 11 (BLKB_MDL_00072686 at -72699). But, incredibly, [redacted]. Curtin Report ¶¶ 50-53; *see also* Ex. 12 (Nov. 5, 2021 Friedberg Tr.) at 193:11-196:20.

B. The data breach: attackers exploit these vulnerabilities to gain access to Blackbaud's networks.

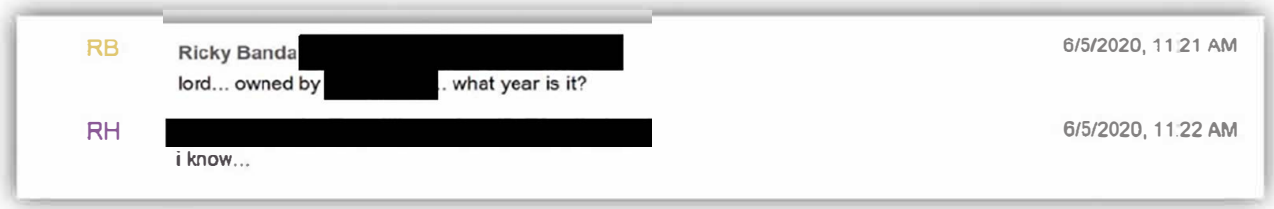
Attackers gained access to Blackbaud's system on February 7, 2020, [redacted] Ex. 13 (BLKB_MDL_00660929). [redacted] *Id.*; Ex. 14 (BLKB_MDL_00208700 at -208702). One month later—in early March 2020—the same [redacted] Ex. 15 (BLKB_MDL_00707292). [redacted] Ex. 16 (BLKB_MDL_00107253 at -107266); Ex. 17 (Wei Tr.) at 56:11-24.

Several months later, on May 14, 2020, Blackbaud detected the data breach. Ex. 18 (Second Amended Response to Interrogatory No. 13) at 55. Members of Blackbaud's threat and detection team quickly pieced together that Blackbaud had [redacted]. On May 21, [redacted] wrote [redacted] Ex. 14 (BLKB_MDL_00208700 at -208703-704) (emphasis added). Another employee, Delores Wei, wrote of the [redacted]

[redacted] Ex. 19 (BLKB_MDL_00303412 at -303428). Of course, that's exactly what happened. She and coworker Carlos Vincent agreed that, due to Blackbaud's cybersecurity "limitations"—[redacted] *Id.*

Blackbaud's subsequent investigation showed that, at each step of the breach, the attackers exploited the same vulnerabilities that Blackbaud employees and outside security consultants had been warning the company's leadership about for years. Blackbaud's former Deputy Chief Information Security Officer, [redacted], summarized the [redacted] Ex. 20 (BLKB_MDL_00054272); Curtin Report ¶¶ 22-23, 39-42, 47, 53-54, 71-74, 94-97. In the days immediately following Blackbaud's detection of the breach, Blackbaud management [redacted] For example, Rich Friedberg wrote that he wanted to identify [redacted] Ex. 21 (BLKB_MDL_00107658 at -107659) (emphasis added).

The attackers themselves confirmed many of these exploited deficiencies. Upon learning from the attackers that they had used the [redacted] exploit, Ricky Banda lamented:



Ex. 22 (BLKB_MDL_00195062 at -195063). The attackers also pointed to [redacted]

[redacted] Ex. 23 (BLKB_MDL_00036274).

C. Blackbaud pays a ransom to unknown hackers [redacted]

On May 20, 2020, the attackers left ransom notes for Blackbaud. One stated that the attackers had [redacted] Ex. 24 (BLKB_MDL_00051018). [redacted] Ex. 25 (BLKB_MDL_00036345). [redacted]" Ex. 24 (BLKB_MDL_00051018).

[redacted]

[5] Only at this point—one week after detecting the breach—did Blackbaud belatedly inform the FBI of the breach. Ex. 18 (Amended Response to Interrogatory No. 14) at 63. [redacted] Ex. 12 (Nov. 5, 2021 Friedberg Tr.) at 58:21-60:3.

[redacted]

After two weeks of negotiations, [redacted] Ex. 23 (BLKB_MDL_00036274 at -36279). Blackbaud paid the ransom on June 3, 2020. [redacted] Ex. 26 (GS-0005824 at -5824 to -5827). [redacted] despite having no way to confirm that these attackers had kept their word, nor any way to police their compliance in the future given their anonymity.

Payment of the ransom was applauded by hackers as a win for the bad guys. In dark web message boards and forums, "various threat actors posted the news of the ransomware payment being paid." Frantz Decl. ¶¶ 64-66. Multiple columns and entries included "clapping emojiis, comments translated from Russian that appear to be associated with Blackbaud . . . such as 'watch your back' and 'don't want to get caught' with payment emoji." *Id.* at ¶ 64. Thus, while Blackbaud was congratulating itself for the decision to pay the ransom, threat actors across the world were joking that such payment provided Blackbaud with [redacted]

D. Blackbaud misled customers and auditors about the attack.

1. Blackbaud issues a belated—and false—disclosure of the breach.

Blackbaud did not notify its customers or the public until July 16, 2020—two months after it learned of the breach. Ex. 18 (Response to Interrogatory No. 12) at 48. Blackbaud posted a notice

on its website, *see* Ex. 1 (PX 25), and [redacted] *E.g.* Ex. 27 (BLKB_MDL_00008839 at -8843). The notice ("Wave 1 Notice") included the following statements:

- "The cybercriminal did not access credit card information, bank account information, or social security numbers."
- "[W]e paid the cybercriminal's demand with confirmation that the copy [of the exfiltrated data] they removed had been destroyed."

These statements were false. At the time, Blackbaud had no basis to represent that the attackers had not accessed sensitive information [redacted] Ex. 28 (Willson Tr.) at 85:12-14 [redacted] It soon emerged that the compromised data included unencrypted Social Security numbers, credit card information, and bank account information. Ex. 18 (Response to Interrogatory No. 12) at 48.

Nor did Blackbaud ever receive "confirmation" the attackers had destroyed the data. Quite the opposite: the attackers ***failed to*** provide a video confirming destruction, as they had agreed to do. Ex. 26 (GS-0005824). Blackbaud internally admitted that "it's not possible to confirm" destruction and that Blackbaud "should not say" it had done so. Ex. 29 (BLKB_MDL_00001313). But it did so anyway, and its misrepresentations remained public for nearly two years: Blackbaud only stopped making this misrepresentation after Plaintiffs filed their Motion for Corrective Notice in early ***2022***. *See* ECF No. 204 (Motion for Corrective Notice).

2. Blackbaud issues a second, still-misleading corrective notice.

After its initial notification to customers, Blackbaud's customers and employees notified Blackbaud's management that the Wave 1 Notice was wrong—Social Security numbers and other sensitive information in unencrypted form had, in fact, been compromised. Ex. 18 (Response to Interrogatory No. 12) at 48-49. At that point, Blackbaud finally began to query the compromised

data for unencrypted sensitive data. Ex. 18 (Response to Interrogatory No. 12) at 48-49. Using SQL queries, Blackbaud was able to readily identify the fields in the compromised databases that contained unencrypted sensitive information. On September 29, 2020—more than two months after its Wave 1 Notices—Blackbaud issued a second notice ("Wave 2 Notice") to over 5,000 customers. *Id.* These notices repeated Blackbaud's assertion that it "paid the cybercriminal's ransomware demand ***with confirmation*** that the copy they removed had been destroyed." *E.g.* Ex. 30 (JKHA 011) (emphasis added).

3. KPMG loses confidence in Blackbaud's integrity and withdraws its security audit reports.

Blackbaud also misled its auditors. KPMG is an accounting firm that, among other things, issues audit reports regarding service organization controls (SOC) for service providers like Blackbaud. [redacted]

[redacted]

The review went poorly for Blackbaud—[redacted] Currigan concluded that Blackbaud's management [redacted]. Ex. 38 (KPMG-BLKB-ESI-0010429); Ex. 31 (Currigan Tr.) at 101:24-103:10, 123:10-17. [redacted] Ex. 31 (Currigan Tr.) at 99:14-100:21; 119:4-9; 125:1-23. [redacted]

[6] [redacted]

[redacted] To date, Blackbaud has not informed either its customers or the regulators of the facts that prompted these extraordinary actions.

E. As a result of the breach, Plaintiffs' and class members' data was placed for sale on the dark web.

The risk of harm to class members—that criminals would traffic in their personal data on the dark web—has materialized. According to the analysis of Plaintiffs' expert, Mary Frantz, cybercriminals have offered class members' data for sale on the dark web in various fora. Frantz Decl. ¶¶ 59-60, 71, 82. For example, personal information for the named Plaintiffs was found in private forums in the year following the data breach (and some named Plaintiffs' information continues to be available), and their information was often found in connection with common threat actors and data repositories. *E.g.* Frantz Decl. ¶¶ 71(g), (h), (k), (m); *id.* ¶¶ 73, 74.

III. CLASS CERTIFICATION IS APPROPRIATE

Class actions are governed by Rule 23 of the Federal Rules of Civil Procedure. Rule 23(a) requires: "(1) the class is so numerous that joinder of all members is impracticable; (2) there are questions of law or fact common to the class; (3) the claims or defenses of the representative parties are typical of the claims or defenses of the class; and (4) the representative parties will fairly and adequately protect the interests of the class." Fed. R. Civ. P. 23(a).

In addition to the prerequisites of Rule 23(a), plaintiffs seeking damages must also satisfy Rule 23(b). Plaintiffs move for certification both under Rule 23(b)(2) and Rule 23(b)(3). The Court may certify a Rule 23(b)(2) class if "the party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole." *Scott v. Fam. Dollar Stores, Inc.*, 2016 WL

9665158, at *7 (W.D.N.C. June 24, 2016) (quoting Rule 23(b)(2)) (granting motion for class certification under both Rule 23(b)(2) and Rule 23)(b)(3)). Rule 23(b)(3) requires that "questions of law or fact common to the class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3).

A. Plaintiffs meet each prerequisite of Rule 23(a).

1. The proposed Classes and Sub-classes are sufficiently numerous.

The proposed Classes and Sub-classes meet the numerosity requirements. "No specified number is needed to maintain a class action." *Brady v. Thurston Motor Lines*, 726 F.2d 136, 145 (4th Cir. 1984) (internal quotation marks omitted). However, "generally speaking, courts find classes of at least 40 members sufficiently large to satisfy the impracticability requirement." *In re Titanium Dioxide Antitrust Litig.*, 284 F.R.D. 328, 337 (D. Md. 2012) (internal quotation marks omitted), *as amended*, 962 F. Supp. 2d 840 (D. Md. 2013). Here, the Classes and Sub-Classes contain millions of members. *See* Curtin Report ¶¶ 169-72. Thus, numerosity is satisfied.

2. Common issues of law and fact exist among class members.

The proposed Classes and Sub-classes also satisfy Rule 23(a)(2)'s commonality requirement. To satisfy this requirement, even "[a] single common question will suffice," *Peters v. Aetna Inc.*, 2 F.4th 199, 242 (4th Cir. 2021), *cert. denied*, 142 S. Ct. 1227 (2022). "[W]hat matters to class certification is the capacity of a class-wide proceeding to generate common *answers* apt to drive the resolution of the litigation." *Id.* (cleaned up) (quoting *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011)). Courts assessing commonality in data breach cases routinely find that common questions regarding a defendant's data security practices satisfy this element. *See, e.g.*, *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 341 F.R.D. 128, 147 (D. Md. 2022); *In re Anthem, Inc. Data Breach Litig.*, 327 F.R.D. 299, 308 (N.D. Cal. 2018); *see also In re TD Bank,*

N.A. Debit Card Overdraft Fee Litig., 325 F.R.D. 136, 152-53 (D.S.C. 2018) (noting that common unlawful conduct or practice could drive common answer to "overarching question" applicable to all class members).

This case is no different. Common questions of law and fact include:

- whether Blackbaud was aware of the vulnerabilities that led to the data breach—including [redacted];
- whether Blackbaud was aware that it, specifically, was vulnerable to attacks because it failed to address these vulnerabilities;
- whether Blackbaud failed to exercise reasonable precautions to prevent the breach;
- whether Blackbaud's inadequate data security caused the data breach;
- whether Blackbaud knew its information security protocols were not in line with industry standards;
- whether Blackbaud's post-breach representations would have been materially misleading or deceptive to a reasonable person;
- whether the data breach exposed class members to a severe, ongoing harm by exposing their data to dark web markets; and
- whether class members suffered lost value of their PII as a result of the data breach.

Answering these questions will "resolve an issue that is central to the validity of each one of the claims in one stroke." *Dukes*, 564 U.S. at 350. *See also* ECF No. 1 (Transfer Order) at 1-2 (identifying "common factual questions" that weighed in favor of centralization, including "Blackbaud's data security practices and whether the practices met industry standards").

3. Plaintiffs' claims are typical of the Classes and Sub-classes.

Plaintiffs satisfy Rule 23's typicality requirement; to do so, "[t]he representative party's interest in prosecuting his own case simultaneously [must] tend to advance the interests of the absent class members." *Dieter v. Microsoft Corp.*, 436 F.3d 461, 466 (4th Cir. 2006). Similarly, "[t]he test for determining typicality is whether the claim or defense arises from the same course of conduct leading to the class claims, and whether the same legal theory underlies the claims or defenses." *Peoples v. Wendover Funding*, 179 F.R.D. 492, 498 (D. Md. 1998). Typicality is not a close call because the named plaintiffs' claims are premised on the same course of conduct and the

same legal theory as all other class members. For example, each class representative alleging negligence alleges the same duty (to protect class members' PII and PHI), the same breach of that duty by Blackbaud (namely, failing to take reasonable steps to protect that data), and the same harms caused by the breach (namely, harm from the ongoing risk of fraud or scams; and loss of value of PII and PHI). The same is true of the class representatives alleging claims under the California CCPA and CMIA, the New York GBL, and the FDUTPA.[7] "In short, the class representatives and the absent members are similarly situated legally and factually because [Blackbaud] pursued the same course of conduct as to all class members." *In re Marriott*, 341 F.R.D. at 149.

4. Plaintiffs and their counsel will adequately represent the Classes and Sub-classes.

Plaintiffs and interim Class Counsel meet Rule 23(a)(4)'s adequacy requirement. The test for adequacy turns on two questions: "(1) whether the named plaintiffs and their counsel have any conflicts of interest with other class members; and (2) whether the named plaintiffs and their counsel will prosecute the action vigorously on behalf of the entire class." *Robinson v. Carolina First Bank NA*, 2019 WL 2591153, at *6 (D.S.C. June 21, 2019). Neither Plaintiffs nor interim Class Counsel have any conflicts with the Class; the class representatives have "suffered the same alleged injuries as the absent class members"—the heightened risk of fraud and scams and the lost market value of their personal information, *see infra* at 32-34—"and the absent class members would receive the same forms of damages should the named Plaintiffs succeed in this litigation." *In re Marriott*, 341 F.R.D. at 151. Plaintiffs have also demonstrated that they will prosecute this

[7] Class representatives Mamie Estes and Kassandre Clayton are representatives (and members) of the CCPA Sub-class; Kassandre Clayton is a representative (and member) of the CMIA Sub-class; Ralph Peragine and Karen Zielinski are representatives (and members) of the New York GBL Sub-class; and Dorothy Kamm is a representative (and member) of the FDUTPA Sub-class.

action vigorously; each has produced documents, responded to written discovery, and sat for deposition. *See* Decl. of Interim Co-Lead Counsel ¶¶ 6, 11.

The Court already concluded in its appointment of Plaintiffs' counsel that these attorneys and their firms satisfy the requirements articulated in Rule 23(g). *See* ECF No. 35. The firms have vigorously and expeditiously prosecuted this case. They have obtained and reviewed hundreds of thousands of documents; taken or defended over 50 depositions; pursued more than 57 non-party subpoenas; briefed three motions to dismiss; engaged in frequent and substantial discovery motion practice with the assistance of Special Master Maura Grossman; and worked with and supervised a team of highly qualified experts. Each of these lawyers has a track record of success in prosecuting complex class actions—including some as lead counsel in other data breach class actions—and is particularly well-suited to serve as Class Counsel. *See* Decl. of Interim Co-Lead Counsel ¶¶ 6-9, 13, 15.

5. Class members may be identified with objective criteria.

Finally, the proposed Classes and Sub-classes are ascertainable. In order to certify a proposed class, the court must be able to "readily identify the class members in reference to objective criteria," *EQT Prod. Co. v. Adair*, 764 F.3d 347, 358 (4th Cir. 2014), and there must be "some administratively feasible way for the court to determine whether a particular individual is a member at some point," *Krakauer v. Dish Network, L.L.C.*, 925 F.3d 643, 658 (4th Cir. 2019) (internal quotation marks and brackets omitted).

First, the proposed Classes and Sub-classes are defined by objective criteria, such as (i) whether an individual's unencrypted data was exposed in the data breach; (ii) which type(s) of unencrypted data for that individual were impacted; (iii) the individual's state of residence; and (iv) whether a class member viewed Blackbaud's post-breach representations regarding the scope of the breach and the "confirmation" of destruction by the cybercriminals (for the New York GBL and

FDUTPA Sub-classes). These are "not matters of belief or states of mind, but objective facts." *In re Marriott*, 341 F.R.D. at 143 (noting that "[w]hether one resides in a [particular] state" is an objective criterion).

Second, Plaintiffs have identified an administratively feasible way to identify Class and Sub-class members using the very data that Blackbaud has identified as having been impacted by the data breach. As described in his expert report, Plaintiffs' expert, C. Matthew Curtin, has been able to identify class members by querying the email addresses present in the data set provided by Blackbaud to Plaintiffs' counsel during discovery.[8] Curtin Report ¶ 141; *id.* at Appendix 4, ¶ 33. Plaintiffs would first perform this step to identify Class and Sub-class members to whom notice should be directed pursuant to Rule 23(c)(2). Mr. Curtin has further developed a method that can query the affected data elements for any class member, which will permit Plaintiffs to identify which Classes and Sub-classes a class member belongs to. Curtin Report ¶¶ 142-43; *id.* at Appendix 4, ¶¶ 36-42. This querying can be accomplished by utilizing a single body of evidence—the compromised Blackbaud databases—in conjunction with basic information provided by class members during the claims process. It will not require individualized adjudications. Rather, the same, common process will be run for each. *Id.* ¶ 147; *id.* at Appendix 4, ¶ 43.

Third, Plaintiffs know their querying method is feasible and reliable because Blackbaud

[8] Specifically, from the set of files that Blackbaud identified as those compromised in the data breach, Blackbaud produced the compromised files for a sample of 100 of its customers that was selected by Plaintiffs. *See* Curtin Report, Appendix 4 at ¶ 10. To select the 100 customers, Plaintiffs' expert statistician, Dr. William Wecker, designed a stratified sample that ensured that customers using all of the affected Blackbaud products were included in the sample and that customers from New York and California—states under whose laws Plaintiffs are asserting claims—were included in the sample. *See* Wecker Report ¶¶ 13-17 & table 1 (describing the five strata from which Dr. Wecker constructed the sample and the reasons for including each stratum). *See also* ECF No. 258 at 1-2 (permitting Plaintiffs to file their class certification brief based upon a 100-customer sample set).

itself used a similar method to identify which specific pieces of unencrypted data were accessed and exfiltrated for each class representative. *See* Curtin Report ¶¶ 148-52. As with Plaintiffs' method, Blackbaud was able to determine which information was impacted for each named Plaintiff by querying Blackbaud's databases using only their names and "basic information" about them.[9] As with Plaintiffs' method, Blackbaud leveraged the "relational" nature of the affected databases to extract the full set of compromised data elements for each class member. Curtin Report ¶¶ 142, 149; *id.* at Appendix 4, ¶¶ 14-17; Ex. 28 (Willson Tr.) at 201:12-14 [redacted][10] [redacted] In other words, Blackbaud employed a single, uniform method of querying its own databases—which did not vary by class member—to identify which data elements were compromised for each class representative.

Blackbaud also used a similar process to that of Plaintiffs in order to identify customers it contacted as part of its "Wave 2" notifications. What notice Blackbaud provided a customer depended on whether or not specific pieces of data were compromised for those customers'

[9] *See* Ex. 18 (Amended Response to Interrogatory No. 10) at 32 ("[O]nce provided with names and basic information for the Plaintiffs, including the identity of the customers Plaintiffs allege they provided their information to, Blackbaud was able to query the relevant customer databases to pull the information belonging to each named Plaintiff stored by its customers.").

[10] [redacted] Ex. 28 (Willson Tr.) at 110:10-111-25, 114:1-3.

constituents. [redacted] Ex. 28 (Willson Tr.) at 153:22-156:6, 159:6-12; Ex. 41 at 12-13 (Response to Interrogatory No. 21) (describing process). [redacted] Ex. 28 (Willson Tr.) at 169:9-14. Blackbaud considers this method reliable and is confident that it accurately and consistently identified those of its customers whose constituents had data exposed in the data breach. Ex. 28 (Willson Tr.) at 53:18-55:17, 98:23-99:12. Indeed, Blackbaud was confident enough that, on the basis of this method, it notified its impacted customers and, in some cases, offered credit and identity monitoring services to those customers so that they could, in turn, offer those services to affected individuals. [redacted] Ex. 28 (Willson Dep.) at 78:13-21. [redacted] *Id.* at 54:10-55:17.

In sum, Plaintiffs have identified a uniform, feasible method using Blackbaud's own databases and basic information from claimants to identify class members and which Sub-classes, if any, they belong to. Blackbaud's own use of substantially identical methods proves that Plaintiffs' method is workable. *See Kelly v. RealPage Inc.*, 47 F.4th 202, 224 (3d Cir. 2022) (rejecting ascertainability challenge where plaintiffs had "identified the records they require, demonstrated they are in [defendant's] possession, and explained how those records can be used to verify putative subclass members"); *In re Marriott*, 341 F.R.D. at 144-45 (finding the defendant's arguments about the unreliability of their database "particularly unavailing here because they used the NDS database to notify the proposed class members of the data breach"); *Soutter v. Equifax Info. Servs., LLC*, 307

F.R.D. 183, 198 (E.D. Va. 2015) (rejecting argument that Plaintiffs' method of ascertaining class members was unworkable where the defendant "ha[d] already proven its ability to determine whether and when a consumer has notified it of an inaccurate Virginia judgment," as required to demonstrate class membership).

The fact that *some* effort will be required to ascertain the members of the Class and Sub-classes does not defeat administrative feasibility. *See In re Marriott*, 341 F.R.D. at 144 (rejecting arguments that method of identifying class members in data breach case using compromised databases, defendant's customer data, and affidavits was not administratively feasible, even though "potential class sizes . . . are large and review of individual files will be required" and identifying class members would "no doubt be time consuming"); *Soutter*, 307 F.R.D. at 197 (same, in a FCRA lawsuit where proposed identification method required using defendant's records and court records; and noting "the majority of sifting in this case will be achieved through dataset searches and other forms of electronic data analysis"); *Moodie v. Kiawah Island Inn Co., LLC*, 309 F.R.D. 370, 376 (D.S.C. 2015) (finding ascertainability satisfied in FLSA action where "[t]he members of Plaintiffs' proposed class are easily identified by reference to Defendant's payroll records and the standard forms it must use to employ H-2B workers during the relevant time period" and noting that the defendant "ha[d] apparently not had any problems" identifying the relevant employees); *Kelly*, 47 F.4th at 224 (holding that putative classes were ascertainable despite fact that plaintiffs' method "require[d] review of individual records with cross-referencing of voluminous data from multiple sources").

Ultimately, "[t]here will always be some level of inquiry required to verify that a person is a member of a class," but a mechanical process of identifying class members "does not require a mini-trial, nor does it amount to individualized fact-finding." *Byrd v. Aaron's Inc.*, 784 F.3d 154,

170-71 (3d Cir. 2015) (cleaned up), *as amended* (Apr. 28, 2015) ("*Carrera* does not suggest that no level of inquiry as to the identity of class members can ever be undertaken. If that were the case, no Rule 23(b)(3) class could ever be certified.").

B. Plaintiffs satisfy the requirements of Rule 23(b).

Additionally, Plaintiffs' claims raise common questions that will predominate over any individual issues, thus satisfying Rule 23(b)(3). While the predominance inquiry "must be 'rigorous' and may 'entail some overlap with the merits of the plaintiff's underlying claim,'" *Amgen Inc. v. Conn. Ret. Plans & Trust Funds*, 568 U.S. 455, 465-66 (2013) (quoting *Dukes*, 564 U.S. at 351), courts ought not "engage in free-ranging merits inquiries at the certification stage," *id.* at 466; *see also Brown v. Nucor Corp.*, 785 F.3d 895, 903 (4th Cir. 2015) ("[A] court should engage the merits of a claim only to the extent necessary to verify that Rule 23 has been satisfied."). In determining predominance, courts compare the common evidence to the individual evidence for the claim as a whole. There is no requirement that common evidence predominate for each element of the claim. *Amgen*, 568 U.S. at 469 ("Rule 23(b)(3), however, does *not* require a plaintiff seeking class certification to prove that each element of her claim is susceptible to class-wide proof.") (emphasis in original) (quotation and brackets omitted).

1. Common evidence will prove Blackbaud's negligence and gross negligence.[11]

Plaintiffs move to certify a nationwide class for their claims of negligence and gross

[11] Under Massachusetts law, gross negligence differs from ordinary negligence only in the extent to which the defendant departs from the standard of care. *See Altman v. Aronson*, 231 Mass. 588, 592 (1919) (noting that "[o]rdinary and gross negligence differ in degree of inattention"). As set out below, proof that Blackbaud failed to take reasonable steps to safeguard class members' information—and the degree to which Blackbaud's conduct was unreasonable—will be proved through common evidence. *See infra* at 24-27. For that reason, common questions predominate for Plaintiffs' gross negligence claims.

negligence. Courts routinely certify negligence claims for class-wide treatment where, as here, the claims are brought under one state's law, common questions of duty and breach center on the defendant's data security practices, and damages can be calculated using a common method. *See, e.g.*, *Smith v. Triad of Alabama, LLC*, 2017 WL 1044692, at *13 (M.D. Ala. Mar. 17, 2017), *on reconsideration in part*, 2017 WL 3816722 (M.D. Ala. Aug. 31, 2017) (certifying Alabama negligence claims arising out of a data breach because the defendant's duty to protect the plaintiffs' information—and breach of the duty—were "common issues susceptible to proof on a class-wide basis" and were "pivotal to the resolution of the litigation" as to all class members).[12]

Under Massachusetts law, a plaintiff alleging negligence "must prove that the defendant owed the plaintiff a duty of reasonable care, that the defendant breached this duty, that damage resulted, and that there was a causal relation between the breach of the duty and the damage." *Jupin v. Kask*, 447 Mass. 141, 146 (2006); ECF No. 265 (holding that Massachusetts law will govern Plaintiffs' negligence claims). As set out below, each element of these claims will be proved through common, class-wide evidence.

i. Plaintiffs will show Blackbaud owed a duty of care to protect class members' PII and PHI through class-wide evidence.

Whether Blackbaud owed a duty of care to class members to reasonably protect their PII and PHI is a common, class-wide question. The existence of a duty is an issue of law that centers on the foreseeability of harm to plaintiffs caused by the defendant's conduct. *See Portier v. NEO Tech. Sols.*, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) (finding a duty of care to safeguard

[12] *See also In re Sonic Corp. Customer Data Breach Litig.*, 2020 WL 6701992, at *6 (N.D. Ohio Nov. 13, 2020), *leave to appeal denied*, 2021 WL 6694843 (6th Cir. Aug. 24, 2021) (certifying negligence claims under Oklahoma law because "common legal negligence standards" governed the plaintiffs' claims, liability could be demonstrated on a class-wide basis, and causation was subject to "generalizable" proof); *In re Target Corp. Customer Data Sec. Breach Litig.*, 309 F.R.D. 482, 487 (D. Minn. 2015) (same, under Minnesota law).

against the misuse of putative class members' PII because "Defendants could be expected to foresee the risk that Plaintiffs' unencrypted PII could be accessed and misused by third party criminals" (citing *Jupin*, 447 Mass. at 147)), *report and recommendation adopted*, 2020 WL 877035 (D. Mass. Jan. 30, 2020). As numerous courts have found—including this Court, in this case—the foreseeable risk that inadequate data security can lead to a cyberattack or data breach supports the existence of a duty of care. *See In re Blackbaud, Inc., Customer Data Breach Litig.*, 567 F. Supp. 3d 667, 679-82 (D.S.C. 2021) (finding that allegations of "Blackbaud's own negligent conduct in creating the risk by failing to use reasonable security measures" supported a duty of care under South Carolina law); *Portier*, 2019 WL 7946103, at *12.

Here, the question of duty centers on Blackbaud's course of conduct, rather than individualized questions relating to class members, because Blackbaud affirmatively undertook to collect and store individuals' PII as part of the services it offered to customers, thereby giving rise to a duty to exercise due care to safeguard the PII.[13] This evidence—which does not require individualized inquiries for each class member—will establish Blackbaud's duty of care as to all

[13] *See* Ex. 18 (Amended Response to Interrogatory No. 11) at 39-42; *Portier*, 2019 WL 7946103, at *11 ("It is reasonable to conclude that NEO Tech's affirmative acts of collecting and storing Plaintiffs' PII gave rise to a duty to exercise due care to safeguard the employees' PII."). These facts do not vary by class member. Additionally, Plaintiffs will show that Blackbaud markets itself as a reliable data security "partner" and understands (and understood prior to the data breach) that if it failed to take reasonable steps to safeguard sensitive data—as it did—that data could be compromised in a cyberattack. *See, e.g.*, Ex. 42 (BLKB_MDL_00105587 at -105598) ("At Blackbaud, your organization's data security is mission-critical, and we take our commitment to protecting it extremely seriously."); Security, https://www.blackbaud.com/security ("Your organization's data security is mission-critical, and we take our commitment to protecting it extremely seriously"; "[O]ur promise to you is that your Blackbaud solution is always secure, protected, and reliable"); Ex. 43 (BLKB_MDL_00208480) ("Cybersecurity Risk Factor" from Blackbaud's 2019 Annual Report: "If the security of our software is breached, we fail to securely collect, store and transmit customer information, or we fail to safeguard confidential donor data, we could be exposed to liability, litigation, penalties and remedial costs and our reputation and business could suffer."); Ex. 44 (BLKB_MDL_00831510 at -831531) ([redacted]; Worley Report ¶¶ 105-06.

class members. *See Smith*, 2017 WL 1044692, at *13 (certifying negligence claims under Alabama law involving theft of PII and PHI because "[t]he questions of duty and breach . . . are common issues susceptible to proof on a class-wide basis."); *In re Target Corp. Customer Data Sec. Breach Litig.*, 309 F.R.D. at 487 (noting that defendant "concede[d] that classwide proof is available as to the existence of a duty and breach of that duty" for negligence claims under Minnesota law).[14]

ii. Class-wide evidence shows that Blackbaud breached these duties.

Likewise, Blackbaud's breach of duty hinges on common proof. Whether Blackbaud breached its duty by failing to take reasonable steps to safeguard class members' data turns on uniform evidence regarding Blackbaud's data security practices. *See In re Anthem, Inc. Data Breach Litig.*, 327 F.R.D. at 312 ("This is the precise type of predominant question that makes class-wide adjudication worthwhile."). Blackbaud's multiple, severe lapses in data security led to the data breach—all of which will be proved through common evidence. *See* Curtin Report ¶¶ 33-97; *id.* at ¶ 7 ("In early 2020, when the threat actors first accessed Blackbaud's systems, Blackbaud's cybersecurity was in an insufficient state to effectively detect, prevent, and respond to . . . compromises [of its systems]."). For example, Blackbaud readily admits that a security vulnerability that it knew about [redacted] allowed the attackers to gain access to Blackbaud's data. *See supra* at 6-7; Ex. 22 (BLKB_MDL_00195062); Ex. 12 (Nov. 5, 2021 Friedberg Tr.) at 197:20-198:6, 210:24-211:2. Furthermore, Blackbaud's failure to implement [redacted]

[14] *See also In re Marriott*, 341 F.R.D. at 169 (certifying issue classes as to duty and breach elements because they could be proved through common evidence, "includ[ing] testimony regarding . . . [defendant's] data security responsibilities, and [defendant's] data security practices related to multifactor authentication, account privileges, monitoring, and encryption"); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 2019 WL 3410382, at *18 (D. Or. July 29, 2019) ("Premera's duty, if any, to protect Sensitive Information, would be owed classwide and whether that duty was breached also would be a class question").

[redacted] which permitted the attackers to remain in Blackbaud's system for several more months, exfiltrating class members' data. *See supra* at 5, 7. [redacted] *See supra* at 8; Ex. 23 (BLKB_MDL_00036274 at -36275) [redacted] Ex. 21 (BLKB_MDL_00107658) [redacted]

In sum, common questions resolved by common proof predominate regarding Blackbaud's failure to exercise due care in handling class members' data prior to the breach.

iii. Causation related to class members' injuries will be demonstrated via common proof.

Finally, Plaintiffs will demonstrate through common evidence that Blackbaud's negligence caused class members' injuries. Causation encompasses (i) legal or "proximate" causation and (ii) factual or but-for causation. *Doull v. Foster*, 487 Mass. 1, 7 (2021).

Whether Blackbaud proximately caused Plaintiffs' injuries centers on the objective question of whether Blackbaud should have reasonably foreseen these harms to class members at the time of its negligent acts. *See Donovan v. Philip Morris USA, Inc.*, 268 F.R.D. 1, 14 (D. Mass. 2010) (holding that "[r]easonable foreseeability is an objective requirement that focuses on what the defendant knew at the time of the alleged wrongdoing" and "can therefore be proven on a class-wide basis"). As set out above, what Blackbaud knew or should have known about its deficient data security practices before the breach will be demonstrated through uniform evidence. *See supra* at 24-26 (discussing class-wide evidence of Blackbaud's duty of care based on the reasonable foreseeability of harm); *see also In re Sonic Corp. Customer Data Sec. Breach Litig.*, 2021 WL

4060369, at *6 (N.D. Ohio Sept. 7, 2021) (denying summary judgment on class-wide negligence claims because "[a] reasonabl[e] jury could find that the hack was a foreseeable consequence of creating and maintaining a vulnerable entry point" and that the ensuing theft of class members' information and their "loss" was foreseeable). For that reason, common issues predominate with respect to proximate causation.

Likewise, but-for causation and the class members' injuries will be demonstrated through class-wide evidence. *See* Ex. A to Decl. of Interim Co-Lead Counsel (Plaintiffs' Proposed Trial Plan) at 7; Worley Report ¶¶ 331; Mangum Report ¶¶ 121-22, 125-26, 132; Frantz Decl. ¶¶ 82-83. Individual trials will not be required to demonstrate that the data breach has exposed class members to significant harm and financial risk, nor would they be required to demonstrate that the breach caused Plaintiffs' damages related to the value of their data.

2. Class members' injuries can be demonstrated via class-wide evidence and redressed via a class-wide damages model.

The data breach caused significant harm to each of the class members, who now face actual, extended risk of fraud and identity theft as well as the lost market value of their personal information. These injuries are not hypothetical; they are supported by common evidence and Plaintiffs' expert reports.

i. Massachusetts law provides that the costs of future monitoring are an appropriate measure of damages for the risk of fraud and identity theft faced by class members.

First, Plaintiffs face actual risk of fraud and identity theft because the personal information exposed in the data breach can be used easily to facilitate fraud through online scams or social engineering schemes.[15] This value to criminals guarantees that the data will be lucrative for

[15] For example, in spear phishing attacks, cybercriminals leverage information about an individual (*e.g.*, that she gives $1000 to a specific charity each year) to create a sophisticated, fraudulent communication to the individual (*e.g.*, a fake email from the charity reminding the individual to

cybercriminals to sell and re-sell on the dark web for years. As Ms. Worley's report describes, there is a robust market for illegally stolen data. *See* Worley Report ¶¶ 306-19. And while information does not need to immediately appear on the dark web to demonstrate injury to the class members,[16] as stated above, Ms. Frantz has discovered that, not only has Blackbaud been a lucrative target for attackers *for years*, but that cybercriminals have, in fact, offered class members' data for sale on the dark web. Frantz Decl. ¶¶ 71, 82. Sensitive information for the named Plaintiffs was found in various private forums within months of the data breach. Moreover, this information was often connected to the same threat actors (*e.g.*, the dark web actor "@maxgood888") and the same data repositories. Frantz Decl. ¶ 71(a), (b), (d), (f), (h); *id.* ¶ 73.[17]

Under Massachusetts law, the risk of fraud and identity theft is an actual, present injury, and class members are entitled to damages for the costs of prospective insurance and credit monitoring. *See Shedd v. Sturdy Mem'l Hosp., Inc.*, 2022 WL 1102524, at *6 (Mass. Super. Apr. 5, 2022) ("Massachusetts has, unlike other jurisdictions, held that costs incurred to mitigate or prevent a substantial risk of harm are recoverable as damages in certain circumstances."); *In re Equifax*, 999 F.3d at 1262 (noting that a settlement with credit monitoring and restoration services for a breach involving Social Security numbers "redresses Plaintiffs' injuries"). This harm flows from the breadth of the Blackbaud data breach and the unique risks posed by the data compromised in the

---

make her annual donation and supplying a link) that can prompt the individual to then provide her credit card information to the criminals. Worley Report ¶ 319.

[16] *See In re Equifax Inc. Customer Data Sec. Breach Litig.*, 999 F.3d 1247, 1262 (11th Cir.), *cert. denied*, 142 S. Ct. 431 (2021), *and* 142 S. Ct. 765 (2022) (holding that "actual identity theft is by no means required when there is a sufficient risk of identity theft" to establish injury-in-fact).

[17] Ms. Frantz noted a number of other troubling issues, including Blackbaud employee credentials found on darknet forums and publicly-available dumps of credential and card information. Frantz Decl. ¶¶ 59-63. Some ongoing vulnerabilities she found were so severe that Ms. Frantz took steps to report them consistent with professional guidelines; for example, Blackbaud has been notified of these issues through counsel. Frantz Decl. ¶ 81.

breach, which will not require individualized, class member-by-class member inquiries to assess. Worley Report ¶¶ 336-38 (describing two tranches of Breach Response Products for class members depending on which identifiable types of personal information were disclosed).

In *Shedd*, class members were victims of a data breach in which their unencrypted PII—including Social Security numbers, credit card information, and other data—was stolen by a cybercriminal and allegedly leaked on the dark web. 2022 WL 1102524, at *2. The defendant moved to dismiss the plaintiffs' negligence claims on the basis that plaintiffs had not pled a cognizable injury. *Id.* at *4. In denying the motion, the court expressly affirmed that the "substantial risk" of "future grave harm" created by the dissemination of an individual's PII on the dark web was a cognizable *present* injury for which future mitigation costs could be recovered as damages:

> Here, the law of damages could not contemplate the reality of 2022, that the theft of highly personal health and financial information and its disbursement on the dark web would create the real risk that a person's identity could be stolen to his or her significant detriment. Vigilant credit monitoring, like the ongoing medical monitoring in *Donovan*, may be the only option available for the Plaintiffs and class members to prevent, mitigate, or ameliorate that future grave harm. I conclude, analogizing to *Donovan*, that ***plaintiffs who allege that their most valuable and personal information has wrongfully been disclosed to unauthorized persons, or stolen in a ransomware attack, and which is likely to remain on the dark web (like minute changes to lung tissue), can state a claim to recover the future costs of credit monitoring (like medical monitoring) to prevent identity theft.***

Id. at *6 (emphasis added). Under *Donovan*, even though a plaintiff's damages remedy encompasses *future* costs that have not yet been incurred, the harm caused by the toxic exposure—or here, exposure to criminals on the dark web—is a current, actual injury for purposes of establishing injury under Massachusetts law. *See Donovan v. Philip Morris USA, Inc.*, 455 Mass. 215, 225-26 (2009). Other courts are in agreement that—in jurisdictions which recognize medical monitoring claims—the present risk of fraud, scams, and identity theft is an injury that may be

remedied by damages for the costs of future credit monitoring.[18]

Here, Plaintiffs will prove that each class member has been injured because each faces a present and "substantial risk of harm" from the risk of scams and fraud resulting from Blackbaud's negligence. *See Shedd*, 2022 WL 1102524, at *6.[19] This risk exists because class members' data will be lucrative for cybercriminals to sell and re-sell on the dark web for years. *See* Frantz Decl. ¶¶ 34-35. Class member data, either individually or, commonly, as large sets of data, can appear for sale on dark web forums for years to come. *See id.*; Worley Report ¶ 312 (describing how "[e]ntire databases are put up for sale to the highest bidder" and showing examples of such sales); Frantz Decl. ¶¶ 48, 59, 68-69 (discussing sales of "data dumps" by dark web actors). As Ms. Frantz's declaration demonstrates, personal information of the named Plaintiffs was found in private forums in the year following the data breach, including in the same data repositories and in connection with the same dark web actors. Frantz Decl. ¶ 71(a), (b), (d), (f), (h); *id.* ¶ 73. In short, class members' "most valuable and personal information has wrongfully been disclosed to unauthorized persons, or stolen in a ransomware attack, and . . . is likely to remain on the dark web." *Shedd*, 2022 WL 1102524, at *6.

The facts supporting the heightened, unique risk of fraud to class members—summarized

[18] *See Stollenwerk v. Tri-W. Health Care All.*, 254 F. App'x 664, 666 (9th Cir. 2007) (discussing a four-part test for an Arizona plaintiff to "recover the costs of *future* medical surveillance" and applying it to plaintiffs alleging the need for credit monitoring (emphasis added)); *Doe v. Sutherland Healthcare Sols., Inc.*, 2021 WL 5765978, at *11 (Cal. Ct. App. Dec. 6, 2021) (unpub.) ("It is an entirely appropriate application of the principles underlying *Potter's* holding that the cost of prospective medical monitoring is cognizable injury in a negligence action to impose responsibility for the cost of credit monitoring services on defendants found liable for a data breach if plaintiffs prove causation."); *Griffey v. Magellan Health Inc.*, 2022 WL 1811165, at *5 (D. Ariz. June 2, 2022) (applying factors from *Stollenwerk* and holding that plaintiffs had adequately pled negligence claims under California law based on purchases of credit monitoring services).

[19] *Cf. In re Equifax*, 999 F.3d at 1262 ("actual identity theft is by no means required when there is a sufficient risk of identity theft").

above and set out in full in Ms. Worley's report, *see* Worley Report ¶¶ 289-319—do not vary by class member. Rather, they center on common evidence relating to the particular risks posed by Blackbaud's negligence for *all* class members that can be redressed via a common damages methodology—that is, remediation through fraud insurance and a monitoring product, consistent with Massachusetts law. Worley Report ¶¶ 331-54; *see Shedd*, 2022 WL 1102524, at *6 (approving class members' "claim to recover the future costs of credit monitoring" to "prevent, mitigate, or ameliorate . . . future grave harm"); *Donovan*, 455 Mass. at 226 (holding that "the present value of the reasonable cost of" monitoring is an element of a claim for monitoring). The prospective costs of this product for the period that class members need it can be quantified in actual damages. Specifically, the analysis of Dr. Mangum demonstrates that these damages can be reliably determined on a class-wide basis. Mangum Report ¶¶ 121-24.

Dr. Mangum's model works as follows: each class and Sub-class member requires one of two data breach response packages depending on which elements of their data were compromised. *See* Worley Report ¶¶ 336-54. As Dr. Mangum shows, once it is determined which insurance product a class member requires,[20] it is simply a matter of multiplication to determine that class member's damages (and the damages of the Classes and Sub-classes as a whole). Mangum Report ¶ 122. In sum, Plaintiffs have a common, class-wide formula for calculating damages under this model which can be applied mechanically for each class member. *See In re Marriott*, 341 F.R.D. at 161-62 (finding that plaintiffs' overpayment damages model, although complex, "applie[d] classwide" and "relie[d] upon the same set of variables" for every damages computation and

[20] Mr. Curtin's method is able to determine, for each Class or Sub-class member, what specific data elements were compromised. Curtin Report ¶ 142. For that reason, identifying which Class and Sub-class members require which insurance package pursuant to Ms. Worley's analysis is feasible. *See* Mangum Report ¶ 123.

therefore was consistent with class-wide treatment).

ii. The value of class members' personal information is also recoverable via common proof and methodologies.

Second, a number of courts—including this one—have recognized that the loss in value of a plaintiff's PII is "cognizable [as] damages in tort actions stemming from data breaches." *In re Blackbaud, Inc., Customer Data Breach Litig.*, 567 F. Supp. 3d at 686 (finding that allegations of "loss of value in [Plaintiffs'] Private Information" satisfied the injury element of negligence under South Carolina law).[21] Here, Plaintiffs will prove that class member PII has actual, monetizable value—[redacted]—which was lost when the data was disclosed without each class member's consent. *See, e.g.*, Ex. 45 (EISEN000341 at -342) (response to CCPA Consumer Access Request of Philip Eisen) at 1-2 (identifying which data relating to Mr. Eisen was sold by Blackbaud in the 12 months preceding his request).[22] [redacted]

[21] *See also In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 600-01 (9th Cir. 2020), *cert.* denied, 141 S. Ct. 1684 (2021) (noting that Plaintiffs had cited to sources demonstrating that browsing histories "carry financial value"); *In re Marriott Int'l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 460-61 (D. Md. 2020) (observing "the growing trend across courts that have considered this issue . . . to recognize the lost property value of this information"); *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *14 (N.D. Cal. Aug. 30, 2017) ("Plaintiffs' allegations that their PII is a valuable commodity, that a market exists for Plaintiffs' PII, that Plaintiffs' PII is being sold by hackers on the dark web, and that Plaintiffs have lost the value of their PII as a result, are sufficient to plausibly allege injury arising from the Data Breaches."); *In re Experian Data Breach Litig.*, 2016 WL 7973595, at *5 (C.D. Cal. Dec. 29, 2016) ("A growing number of federal courts have now recognized Loss of Value of PII as a viable damages theory." (citing *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *43 (N.D. Cal. May 27, 2016)).

[22] Blackbaud's CCPA Policy states outright that Blackbaud sells individuals' data to its nonprofit customers. *See* Ex. 46 (PX 112) at 2 (California Consumer Privacy Act Policy) (stating that Blackbaud sells consumer data to "nonprofit organizations and one agency that serves the nonprofit community in direct marketing prospect acquisition" and giving California consumers the ability to opt out of having their data sold).

[redacted] *See, e.g.*, Ex. 47 (Van Diest Tr.) at 85:10-15 ([redacted] Ex. 48 (BLKB_MDL_01098749) [redacted] *See also* Mangum Report ¶¶ 91-94, 96-97 & figs. 9-10, 12-13 (summarizing Blackbaud's prices for specific data elements). [redacted]

Evidence that class members' PII was monetized and had value in an actual market supports the fact that they are injured. *See In re Am. Med. Collection Agency, Inc. Customer Data Sec. Breach Litig.*, 2021 WL 5937742, at *10 (D.N.J. Dec. 16, 2021) (explaining that cases where loss of value of PII is recognized as a cognizable injury "involved circumstances where the defendants collected information that was itself monetized and used for commercial purposes"); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 2019 WL 3410382, at *11, *18 (certifying a settlement class and finding that plaintiffs' "classwide damages [model] for loss of value of Sensitive Information" "involved classwide proof and appl[ied] uniformly" to class members). Moreover, evidence that class members' PII had actual value—which includes Blackbaud's own pricing documents, among other things—is common across class members and will not require individualized inquiries. *See* Mangum Report ¶¶ 91-94, 96-97 & figs. 9-10, 12-13 (describing the Blackbaud documents which demonstrate the market value of each data element); *see also In re Marriott*, 341 F.R.D. at 154 (noting that a model based on the defendant's "own valuation of the

monetary value of . . . customers' PII" could establish not only class-wide injury, but class-wide *damages*). As Dr. Mangum describes in his expert report, the value of each class member's personal information is formulaic and based upon class-wide proof. Mangum Report ¶ 126. To determine a particular class member's overall lost value of PII, Dr. Mangum proposes two, alternative damages methodologies. First, Plaintiffs need only identify the data elements relating to the class member that were exposed in the breach, look up the value of each of those elements, and add them together. Mangum Report ¶¶ 127-31. Alternatively, Mr. Mangum proposes that the value of the data may be determined based upon dark web bulk sales, which provide a value for data regardless of the specific data elements included. Mangum Report ¶¶ 132-33. Regardless of which methodology is employed for this specific purpose, they are both based upon the well-accepted principle that data has value.

3. Plaintiffs' CCPA claims will be resolved via common proof.

Plaintiffs' claims under the CCPA will not require individualized proof. "The CCPA provides a private right of action for actual or statutory damages to any consumer whose [1] nonencrypted and nonredacted personal information is subject to an unauthorized access and exfiltration, theft, or disclosure [2] as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." *In re Blackbaud, Inc., Customer Data Breach Litig.*, No. 20-MN-02972-JMC, 2021 WL 3568394, at *4 (D.S.C. Aug. 12, 2021) (cleaned up) (numbering added).

First, Plaintiffs can identify through common evidence which class members' "nonencrypted and nonredacted personal information was subject to an unauthorized access and exfiltration, theft, or disclosure." *Id.* Under the CCPA, "personal information" means "[a]n individual's first name or first initial and the individual's last name in combination with any one or

more of the following data elements,[23] when either the name or the data elements are not encrypted or redacted." Cal. Civ. Code § 1798.81.5(d)(1)(A). As discussed with regard to ascertainability, Plaintiffs can determine for each class member which specific pieces of information were (i) accessed and exfiltrated, stolen, or disclosed; and (ii) were unredacted, *see supra* at 19-20, which therefore enables members of the CCPA Sub-class to be readily identified. *See* Curtin Report ¶ 167; Appendix 13. Blackbaud itself has demonstrated that CCPA Sub-class members can be identified. *See* Ex. 40 (Second Revised Ex. B to Defendant's Fact Sheet) at 6 [redacted]

Second, Blackbaud's "violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect [Plaintiffs'] personal information" parallels Blackbaud's breach of its common-law duties. *See supra* at 26-27. At trial, Plaintiffs' evidence that Blackbaud violated this duty and caused the data breach will focus on Blackbaud's course of conduct in failing to adequately protect class member data—not on individualized facts that vary by class member. *See supra* at 26-27. Common questions thus predominate with regard to Plaintiffs' CCPA claims.

4. Plaintiffs' CMIA claims are also triable with common proof.

Common issues also predominate regarding Plaintiffs' CMIA claims, which will be established through class-wide proof. The CMIA prohibits the "negligent[] release" of a person's "medical information." Cal. Civil Code § 56.36(b), (c); *see id.* § 56.101(a) (subjecting health care

[23] These data elements include, among other things, a person's Social Security number, driver's license number, account number or credit or debit card number, medical information, and health insurance information. Cal. Civ. Code § 1798.81.5(d)(1)(A).

providers who negligently store "medical information" to liability under Section 56.36). To show a "release" of information, a plaintiff must "prove that the records . . . were actually viewed by an unauthorized person." *Sutter Health v. Superior Ct.*, 227 Cal. App. 4th 1546, 1555 (Cal. Ct. App. 2014).

As a threshold matter, Plaintiffs can readily identify the class members belonging to this Sub-class. Under the CMIA, "medical information" is "any individually identifiable information . . . regarding a patient's medical history, mental or physical condition, or treatment." Cal. Civil Code § 56.05(*i*).[24] Plaintiffs' querying method can identify which class members had data elements regarding their "medical history, mental or physical condition, or treatment" compromised in the breach. *See* Curtin Report ¶ 166; Appendix 13 (identifying which data fields in Blackbaud's databases reflect information about an individual's medical history, condition, or medical treatment). This method can further identify which claimants had "medical information" disclosed in conjunction with personal identifying information such as a name, address, email address, telephone number, or SSN, as required by the CMIA. *See* Cal. Civil Code § 56.05(*i*). This method is algorithmic and does not require individualized proof for each class member. *See* Curtin Report ¶¶ 147, 166; Appendix 13.

Common evidence also shows that Sub-class members' medical information was [redacted]

[24] "'Individually identifiable' means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the identity of the individual." *Id.*

[redacted] goes well beyond the circumstantial evidence other courts have found sufficient to plead and prove a CMIA claim.[25] Even though Blackbaud will dispute these facts at trial, "[t]he question of whether a third party (the alleged hackers) accessed the data is also a common question, because it involves common evidence regarding whether data was exported or exfiltrated from [Blackbaud's] servers." *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 2019 WL 3410382, at *20 (certifying CMIA claims for settlement because "common issues of law and fact predominate[d]").

5. Plaintiffs' GBL claims will also rely upon common evidence.

To prevail on a GBL claim, a plaintiff must prove "(1) the defendant's conduct was consumer-oriented; (2) the defendant's act or practice was deceptive or misleading in a material

[25] *See Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 924 (S.D. Cal. 2020) ("Given that Plaintiffs allege that Inmediata posted their information on the internet, making it searchable, findable, viewable, printable, copiable, and downloadable by anyone in the world with an internet connection, (¶¶ 7-8), it can be reasonably inferred that someone viewed it."); *Falkenberg v. Alere Home Monitoring, Inc.*, 2015 WL 800378, at *4 (N.D. Cal. Feb. 23, 2015) (finding plausible the inference that an unauthorized party "actually viewed" compromised medical information based on subsequent identity theft).

way; and (3) the plaintiff suffered an injury as a result of the deception." *Himmelstein, McConnell, Gribben, Donoghue & Joseph, LLP v. Matthew Bender & Co., Inc.*, 37 N.Y.3d 169, 176 (2021).

For the New York GBL Sub-class, each of these elements is subject to common proof. *First*, Blackbaud's post-breach representations were published on its website and transmitted through its customers, and were therefore "consumer-oriented"—that is, "directed to the consuming public and the marketplace." *Id.* at 177. Blackbaud told *the public*, not simply a private counterparty, that the cybercriminals did not access credit card information, bank account information, or social security numbers and that it had received confirmation the data had been "destroyed."[26] In the same communications, Blackbaud omitted and concealed that it had not [redacted] and omitted that it had not performed an adequate investigation into the dissemination of the information—or even looked at the compromised data before making the announcement. These representations and omissions do not vary by class member. *See* Zielinski Decl. ¶¶ 4, 6-8; Peragine Decl. ¶ 5.

Second, whether Blackbaud's false statements and omissions were "misleading in a material way" requires no individual inquiry because the legal standard is objective. Here, Blackbaud's statements were "likely to mislead a reasonable consumer acting reasonably under the circumstances," *Dupler v. Costco Wholesale Corp.*, 249 F.R.D. 29, 43 (E.D.N.Y. 2008) (certifying GBL claims under Section 349), because they were false and misleading. *See* Worley Report ¶¶ 151, 157-61. Again, no individualized proof will be required.

Third, Sub-class members suffered further, ongoing injury as a result of Blackbaud's

[26] *See* Ex. 1 (PX 25); Blackbaud, *Security Incident*, https://web.archive.org/web/20200719170537/https://www.blackbaud.com/securityincident (July 1, 2020 archive of website); Ex. 50 (BLKB_MDL_01100376) (July 27, 2020 letter to Blackbaud from New York Attorney General inquiring about these representations).

misrepresentations and omissions due to the ongoing risk they faced due to the exposure of their information to criminals without having the information necessary to protect themselves. *See In re GE/CBPS Data Breach Litig.*, 2021 WL 3406374, at *9 (S.D.N.Y. Aug. 4, 2021) (finding that "ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm" was a cognizable harm under New York law).[27] Blackbaud told its customers and the public in mid-July 2020 that "[t]he cybercriminal did not access credit card information, bank account information, or social security numbers" and Blackbaud had "confirmation" that the exfiltrated data had been "destroyed." Ex. 1 (PX 25). At the same time it was falsely telling customers and consumers not to worry about their data, however, that same data was being offered for sale on the dark web by cybercriminals. Frantz Decl. ¶¶ 59-63, 68, 71, 82. Had Blackbaud not painted a false picture of what data had been compromised, downplayed the risks created by its disclosure, and omitted to inform class members that it had failed to even investigate whether whole categories of sensitive data had been exposed—and thereby deprived them of information necessary to understand the risks created by Blackbaud—Blackbaud's customers and Sub-class members could have taken steps to mitigate the risk of fraud and the loss of value of their PII/PHI. *See* Worley Report ¶ 154 ("explaining that "Blackbaud unreasonably assured the [Social Good Entities], the public, and the Class that there was little risk of harm from potential misuse of the unlawfully accessed and likely exfiltrated Personal Information").

6. Statutory damages can be computed without individualized inquiries.

Plaintiffs' claims under the CMIA, CCPA, and New York GBL permit statutory damages.[28]

[27] While the Court in *In re GE/CBPS Data Breach Litigation* was assessing injury in the context of a negligence claim, the analysis remains the same.

[28] *See* Cal. Civ. Code § 1798.150(1) (CCPA) ("damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater"); Cal. Civ. Code § 56.36(b) (CMIA) ("nominal damages of

Determining damages for each of these Sub-classes only requires multiplying the number of incidents or violations of each statute by the respective statutory damages amount. *See* Mangum Report ¶¶ 135, 140, 146. Thus, courts routinely find that statutory damages are amenable to class-wide determination. *See Stillmock v. Weis Markets, Inc.*, 385 F. App'x 267, 273 (4th Cir. 2010) (holding that "individual statutory damages issues are insufficient to defeat class certification under Rule 23(b)(3)" and vacating denial of certification on that basis); *Sykes v. Mel S. Harris & Assocs. LLC*, 780 F.3d 70, 87 (2d Cir. 2015) ("It is not disputed that statutory damages under GBL § 349 can be assessed on the basis of common proof, as they are capped at $50."); *In re Marriott*, 341 F.R.D. at 164 (finding predominance requirement satisfied as to class-wide statutory damages under Section 349 of the GBL).

7. Plaintiffs' FDUTPA claims for injunctive and declaratory relief will rely upon the same types of class-wide proof.

Finally, Plaintiffs' claim for injunctive and declaratory relief under the FDUTPA should proceed on a class-wide basis. "A consumer claim for damages under FDUTPA has three elements: (1) an objectively deceptive act or unfair practice; (2) causation; and (3) actual damages." *Desue v. 20/20 Eye Care Network, Inc.*, 2022 WL 796367, at *10 (S.D. Fla. Mar. 15, 2022). But "[i]n the absence of actual damages, the FDUTPA permits any 'aggrieved party' to pursue injunctive relief." *In re Am. Med. Collection Agency*, 2021 WL 5937742, at *29.

Evidence of Blackbaud's deceptive acts will be uniform across class members. As explained regarding Plaintiffs' New York GBL claims, Blackbaud falsely told Sub-class members that no sensitive information (such as SSNs) had been disclosed, it had received "confirmation" the data

---

one thousand dollars"); N.Y. Gen. Bus. Law § 349(h) ("[A]ny person who has been injured by reason of any violation of this section may bring an action in his own name to enjoin such unlawful act or practice, an action to recover his actual damages *or fifty dollars*, whichever is greater, or both such actions.") (emphasis added).

had been destroyed, and it had "no reason to believe" the data "was or will be misused" or "will be disseminated or otherwise made available publicly." *See* Ex. 1 (PX 25); Kamm Decl. ¶¶ 5-6; *supra* at 10-12. Proof of the deceptiveness of these statements will not vary across Sub-class members.

Similarly, Plaintiffs' evidence that they are "aggrieved parties" will not require individualized inquiries. A party is "aggrieved" when "the deceptive conduct alleged has caused a non-speculative injury that has affected the plaintiff beyond a general interest in curbing deceptive or unfair conduct." *Superior Consulting Servs., Inc. v. Shaklee Corp.*, 2017 WL 2834783, at *7 (M.D. Fla. June 30, 2017). Here, class members have all suffered a heightened and severe risk of fraud, scams, and social engineering. Worley Report ¶¶ 289-319. As Ms. Worley's analysis demonstrates, this injury can be demonstrated through class-wide evidence. This injury suffices to show that members of the Sub-class are "aggrieved" parties. *See Farmer v. Humana, Inc.*, 582 F. Supp. 3d 1176, 1191-92 (M.D. Fla. 2022) ("finding that a "substantially increased risk of fraud" and "identity theft" were sufficient to support a claim for injunctive relief under FDUTPA).

Injunctive relief is appropriate pursuant to Plaintiffs' FDUTPA claim because Blackbaud "has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief . . . is appropriate respecting the class as a whole." Fed. R. Civ. P. 23(b)(2). "When a class seeks an indivisible injunction benefiting all its members at once, there is no reason to undertake a case-specific inquiry into whether class issues predominate or whether class action is a superior method of adjudicating the dispute." *Dukes*, 564 U.S. at 362-63. Accordingly, the "key to the (b)(2) class is 'the indivisible nature of the injunctive or declaratory remedy warranted—the notion that the conduct is such that it can be enjoined or declared unlawful only as to all of the class members or as to none of them.'" *Id.* at 360 (quoting Nagareda, *Class Certification in the Age of Aggregate Proof*, 84 N.Y.U. L. REV. 97, 132 (2009)).

Here, Plaintiffs' injunctive relief claim meets the Rule 23(b)(2) standard because Blackbaud acted in a manner common to the class and failed to protect the class members' personal information by employing reasonable data security measures. Blackbaud subjected all class members' personal information to the same security vulnerabilities; class members' personal information was compromised as a result of those vulnerabilities; Blackbaud continues to hold itself out as a data security leader and to collect and house class member personal information; and Blackbaud remains deficient when it comes to protecting that personal information.[29] Injunctive relief is thus needed to remediate Blackbaud's inadequate on-going security, which uniformly applies to all class members.[30] Mr. Curtin has set forth the inadequacies in Blackbaud's adopted remediations and the security controls needed to protect class members' personal information now and in the future. Curtin Report ¶¶ 123-38. And Ms. Frantz has demonstrated that such security measures are needed because Blackbaud continues to have ongoing security vulnerabilities. Frantz Decl. ¶¶ 81.

Given Blackbaud's inadequate cybersecurity, injunctive relief pursuant to Rule 23(b)(2) is necessary to ensure that class member data is protected. *See Adkins v. Facebook, Inc.*, 424 F. Supp. 3d 686, 697-99 (N.D. Cal. 2019) (certifying Rule 23(b)(2) class seeking declaration of insufficient data security practices and corresponding injunctive relief).

C. Class treatment is superior to other ways of adjudicating the controversy.

Given the overarching common questions of liability, proceeding as a class action is "superior to other available methods for fairly and efficiently adjudicating the controversy." Fed.

[29] Injunctive relief is also available and can be resolved on a class-wide basis for the respective Classes' and Sub-classes' claims under Massachusetts common law; the CCPA, *see* Cal. Civil Code § 1798.150; and the New York GBL.

[30] As noted above, Ms. Frantz identified certain ongoing vulnerabilities with Blackbaud's systems that were so severe that she took steps to report them consistent with professional guidelines; for example, Blackbaud has been notified of these issues through counsel. Frantz Decl. ¶ 81.

R. Civ. P. 23(b)(3). Factors a district court should consider include: "(A) the class members' interest in individually controlling the prosecution or defense of separate actions; (B) the extent and nature of any litigation concerning the controversy already begun by or against class members; (C) the desirability or undesirability of concentrating the litigation of the claims in the particular forum; and (D) the likely difficulties in managing the class action." Fed. R. Civ. P. 23(b)(3)(A)-(D).

First, most class members have a *de minimis* interest in individually controlling the prosecution of separate actions "because the monetary value of their damages would be dramatically outweighed by the cost of litigating an individual case." *In re TD Bank, N.A. Debit Card Overdraft Fee Litig.*, 325 F.R.D. at 162. Under any of the damages models described above, this is a negative-value case. *See supra* at 28-35. "In other words, for most class members the only realistic alternative to a class action is no action at all." *Id.*; *see also Stillmock*, 385 F. App'x at 274 (concluding that recovery of $1,000 in statutory damages and attorneys' fees would be too small for plaintiffs to pursue individual actions).

Second, "[b]ecause numerous putative class action lawsuits based on the same facts and containing substantively identical claims have already been filed against Defendant[], the Judicial Panel on Multidistrict Litigation has seen fit to consolidate the handling of those common claims in this Court." *In re Marriott*, 341 F.R.D. at 165 (internal quotation marks omitted). This factor also weighs in favor of proceeding on a class-wide basis.

Finally, because common issues predominate with respect to Plaintiffs' claims, individual manageability issues will not overwhelm a class proceeding. *See id.* at 166-67. And the difficulties of managing a class action pale in comparison with the alternative—thousands of individual lawsuits. *See id.* at 167 (in assessing superiority, "courts compare the effectiveness of a class action with the alternatives"); *Comer v. Life Ins. Co. of Alabama*, No. C/A 0:08-228-JFA, 2010 WL

233857, at *9 (D.S.C. Jan. 14, 2010) ("The dozens of lawsuits that would result from denying certification would burden the court system with an identical question of liability under the contract."). For those reasons, proceeding as a class action is superior to the alternatives.

IV. CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that this Court: (1) grant Plaintiffs' Motion to Certify the Class; (2) appoint Plaintiffs as Class representatives; and (3) appoint those previously selected as interim Co-Lead Class Counsel to be co-Lead Class Counsel.[31]

[31] Plaintiffs further request that the Court select those previously appointed to the Plaintiffs' Steering Committee (*see* ECF No. 35) to continue in that capacity.

Dated: December 16, 2022

Respectfully submitted,

/s/ Krysta Kauble Pachman

Krysta Kauble Pachman
SUSMAN GODFREY LLP
1900 Avenue of the Stars, Suite 1400
Los Angeles, CA 90067
Tel: (310) 789-3100
Fax: (310) 789-3150
Email: kpachman@susmangodfrey.com

Marlon E. Kimpson (SC Bar No. 17042)
MOTLEY RICE LLC
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Tel.: (843) 216-9000
Fax: (843) 216-9027
Email: mkimpson@motleyrice.com

Amy E. Keller
DICELLO LEVITT LLC
Ten North Dearborn Street, Sixth Floor
Chicago, IL 60602
Tel: (312) 214-7900
Fax: (312) 253-1443
Email: akeller@dicellolevitt.com

Harper Segui
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLP
825 Lowcountry Blvd., Suite 101
Mount Pleasant, SC 29464
Tel: (919) 600-5000
Fax: (919) 600-5035
Email: hsegui@milberg.com

Plaintiffs' Co-Lead Counsel

Gretchen Freeman Cappio
KELLER ROHRBACK L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel.: (206) 623-1900
Fax: (206) 623-3384
Email: gcappio@kellerrohrback.com

Chair of Plaintiffs' Steering Committee

Desiree Cummings
ROBBINS GELLER RUDMAN & DOWD LLP
420 Lexington Avenue, Suite 1832
New York, NY 10170
Tel: (212) 432-5100
Email: dcummings@rgrdlaw.com

Melissa Emert
KANTROWITZ, GOLDHAMMER & GRAIFMAN, PC
747 Chestnut Ridge Road
Chestnut Ridge, NY 10977
Tel: (866) 574-4682
Fax: (845) 356-4335
Email: memert@kgglaw.com

Kelly Iverson
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Email: kiverson@lcllp.com

Howard Longman
LONGMAN LAW, P.C.
354 Eisenhower Parkway, Suite 1800
Livingston, New Jersey 07039
Tel: (973) 994-2315
Fax: (973) 994-2319
Email: Hlongman@longman.law

Douglas McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue NW
East Tower, 5th Floor
Washington, DC 20005
Tel: (202) 408-4600
Fax: (202) 408-4699
Email: dmcnamara@cohenmilstein.com

Melissa Weiner

PEARSON, SIMON & WARSHAW, LLP
800 LaSalle Avenue, Suite 2150
Minneapolis, MN 55402
Tel: (612) 389-0600
Fax: (612) 389-0610
Email: mweiner@pswlaw.com

Plaintiffs' Steering Committee

Catherine H. McElveen
MCCULLEY MCCLUER LLC
701 East Bay Street, Suite 411
Charleston, SC 29403
Tel: (843) 444-5404
Fax: (843) 444-5408
Email: kmcelveen@mcculleymccluer.com

Plaintiffs' Liaison Counsel