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

ALEXANDRA L. MITCHELL, individually and on behalf of all others similarly situated,	:	
Plaintiff,	:	**CIVIL ACTION NO.:**
v.	:	
BLACKBAUD, INC.,	:	
Defendant.	:	

CLASS ACTION COMPLAINT

1. Plaintiff Alexandra L. Mitchell, individually and on behalf of all others similarly situated ("Plaintiff Mitchell" or "Plaintiff") brings this action against Defendant Blackbaud, Inc. ("Blackbaud" or "Defendant") seeking monetary damages, restitution, and/or injunctive relief for the Class, as defined below. Plaintiff makes the following allegations upon information and belief, the investigation of their counsel, and facts that are a matter of public record.

NATURE OF THE ACTION

2. The release, disclosure, and publication of sensitive, private data can be devastating. Not only is it an intrusion of privacy and a loss of control, but it is also a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[1] A data breach can have grave consequences for victims for years after the actual date of the breach—with the obtained information thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, obtain government benefits, or obtain driver's licenses all

[1] Dave Maxfield & Bill Latham, *Data Breaches Perspectives from Both Sides of the Wall*, S.C. Law (May 2014).

in the victims' names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

3. South Carolina cloud computing vendor Blackbaud was keenly aware of the risk of cyberattacks and breach of its customers' confidential data. In fact, Defendant has stated that the secure collection, storage, and transmission of confidential data is fundamental to its business.[2] Defendant likewise knew it was vulnerable to cyberattacks, identifying security breach or intrusion and loss or theft of confidential donor data as a vulnerability in its Annual Report filed with the U.S. Securities and Exchange Commission ("SEC"). In that same document, Defendant also acknowledged its obligation of notification in the event of a breach.[3]

4. Yet, in February 2020, the same month Defendant acknowledged this risk, it failed to detect a ransomware attack on its server. For three and a half months, between February 7, 2020 and May 20, 2020, cyber criminals orchestrated what Defendant has downplayed as a "security incident" when they infiltrated the Defendant's inadequately protected computer networks, thereby gaining access to and copying data and servers managed, maintained, and secured by Defendant (the "Data Breach").[4]

5. In a typical ransomware attack, one is "locked out" of one's data or system by a malicious actor until a ransom is paid. Once the ransom is paid, access is granted. But that is not all that transpired here. Rather, cyber criminals successfully breached Defendant's network and exfiltrated (i.e., stole) data from it. Defendant admitted that data was exfiltrated during the "security incident," in its filing to the SEC on September 29, 2020, where it states: "[f]urther

---

[2] *See* Blackbaud, Inc., Annual Report ("2019 Form 10-K") at 20 (Feb. 20, 2020), https://investor.blackbaud.com/static-files/9cd70119-4e13-4d47-b068-3c228c580417.
[3] *Id.*
[4] Blackbaud, Inc., Form 8-K at 2 (Sept. 29, 2020), https://investor.blackbaud.com/static-files/58a4ae64-afc5-45f7-81df-69dfc93888fc.

forensic investigation found that for some of the notified customers, the cybercriminal may have accessed some unencrypted fields intended for bank account information, [S]ocial [S]ecurity numbers, usernames and/or passwords."[5]

6. Defendant's servers contained Personally Identifiable Information ("PII"), Protected Health Information ("PHI"), and "Personal Information," as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2), (collectively, "Private Information") of individual consumers, including Plaintiff. As a result of this Data Breach, Plaintiff has and will suffer ascertainable losses in the form of out-of-pocket expenses and/or the value of her time incurred to remedy or mitigate the effects of the attack. Additionally, Plaintiff and Class Members' sensitive Private Information—which was entrusted to Defendant—was not only compromised and unlawfully accessed as a result of the Data Breach and made subject to unlawful use by unknown parties, but also obliged some Class Members to purchase mitigating identity protection services. Information compromised in the Data Breach included a "copy of a subset of information" retained by Defendant, including name(s), addresses, phone numbers, Social Security numbers and other Private Information.[6]

7. A true and accurate copy of the Notice of Data Breach ("Notice") mailed to Plaintiff (in her maiden name), by the school through which Blackbaud obtained her Private Information, is attached hereto as Exhibit A. Defendant's own statement regarding the breach is available on its website.[7] Contrary to the representations by Defendant, as reflected in its statement and the Notice

[5] *Id.*
[6] *Id.*
[7] Blackbaud, Inc., *Security Incident* (updated Sept. 29, 2020), https://www.blackbaud.com/securityincident.

Plaintiff received, credit card numbers, bank account numbers, and/or other Private Information may have been compromised.

8. Plaintiff brings this class action lawsuit in order to (1) address Defendant's inadequate safeguarding of Class Members' Private Information, which Defendant managed, maintained, and secured; (2) address Defendant's failure to provide timely and adequate notice to Plaintiff that her information had been subject to the unauthorized access of an unknown third-party; (3) address Defendant's failure to identify all information that was accessed; and (4) address Defendant's failure to provide Plaintiff with adequate redress for the Data Breach or act to mitigate her damages.

9. Defendant caused substantial harm and injuries to Plaintiff and Class Members across the United States by, *inter alia*, failing to: (1) timely implement adequate and reasonable measures to ensure Plaintiff's and Class Members' Private Information was properly protected; (2) timely detect the Data Breach; (3) take adequate steps to prevent and stop the Data Breach; (4) disclose the material facts that it did not have adequate systems and security practices to safeguard Plaintiff's and Class Members' Private Information; (5) honor its repeated promises and representations to protect the Plaintiff's and Class Members' Private Information; (6) identify all information that was accessed; (7) maintain its computer network in a condition to adequately protect against ransomware attacks or other cyberattacks; (8) provide timely and adequate notice of the Data Breach; (9) properly monitor the computer network and systems that housed Plaintiff's and Class Members' Private Information; (10) implement appropriate policies to ensure secure communications of Private Information to Defendants' clients; (11) properly train employees regarding preventing and responding to ransomware attacks; and (12) provide Plaintiff and Class Members with adequate redress for the Data Breach.

10. Had Defendant properly monitored its network, security, and communications, it would have discovered the cyberattack sooner or prevented it altogether. In fact, Defendant has announced it has "already implemented changes to prevent this specific issue from happening again."[8] Had the necessary changes been made previously, this incident would not have happened, and Plaintiff's Private Information would not have been accessed.

11. Plaintiff's Private Information is now at risk because of Defendant's negligent conduct as the Private Information that Defendant collected and maintained is now in the hands of cyber criminals. Defendant cannot reasonably maintain that the data thieves destroyed the extracted data simply because Defendant paid the ransom and the perpetrators stated the copy was destroyed. In fact, the Notice provided by the school through which Defendant obtained Plaintiff's data advised that Class Members should monitor their own credit records, beware of suspicious account activity, and notify the school or non-profit of suspicious activity related to his or her credit record.[9] Despite this, Defendant offered Class members little in the way of redress, such as credit monitoring or proactive fraud protection and no financial support for time or expenses incurred in the event of fraud.

12. As a result of the Data Breach, Plaintiff and Class Members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud and identity theft, for a period of years, if not decades. Beyond the anemic 24 months of "Single Bureau Credit Monitoring" offered by Defendant (and only if enrollment occurs within 90 days of Notice), Class Members, must now and in the future closely monitor their financial accounts to guard against identity theft, at their own expense. Consequently, Plaintiff and Class Members will incur on-

[8] *Id.*
[9] *See* Ex. A.

going out-of-pocket costs for, e.g., purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. By this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly-situated individuals, whose Private Information was accessed during the Data Breach.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits of its data security systems, and provision adequate, robust credit monitoring and restoration services funded by Defendant.

15. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) intrusion upon seclusion or common law breach of privacy, (iii) negligence *per se*, (iv) breach of implied contract, and (vi) violations of Colorado state privacy protection and consumer protection statutes.

PARTIES

16. Plaintiff Alexandra L. Mitchell (formerly Alexandra L. Wedderstrand) is a resident and citizen of Colorado Springs, El Paso County, Colorado. Plaintiff Mitchell is acting on her own behalf and on behalf of others similarly situated. Plaintiff Mitchell's Private Information was breached during the Data Breach.

17. Defendant Blackbaud is a Delaware corporation with its principal place of business located on Daniel Island, Charleston County, South Carolina.

18. Defendant manages, maintains, and provides cloud computing software, services and cybersecurity for the data obtained by its clients who are, *inter alia*, hospitals, non-profit

companies and schools,[10] including St. Andrew's Episcopal School, which maintained Plaintiff's Private Information—the data that was breached in this instance. Defendant has more than 25,000 clients in more than 60 countries.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, 28 U.S.C. § 1711, *et seq.*, because at least one member of the Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

20. This Court has personal jurisdiction over this action because Defendant maintains its principal place of business in this District, has sufficient minimum contacts with this District and has purposefully availed itself of the privilege of doing business in this District such that it could reasonably foresee litigation being brought in this District. This Court also has diversity jurisdiction over this action. 28 U.S.C. § 1332(a).

21. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) because Defendant resides in this District.

DEFENDANT BLACKBAUD

22. Since originally incorporating in 1982, Defendant has become "the world's leading cloud software company powering social good."[11] It provides cloud software, services, expertise and data intelligence which its clients use for administration, fundraising, and financial

[10] Blackbaud, Inc., *About Blackbaud*, https://www.blackbaud.com/company (last visited Jan. 12, 2021).
[11] 2019 Form 10-K at 3.

management.[12] Some of Defendant's most popular products are "Raiser's Edge" and "Financial Edge."[13]

23. Defendant is a publicly traded company with clients that include "nonprofits, foundations, corporations, education institutions, healthcare institutions, and the individual change agents who support them."[14]

24. Defendant reported that at the end of 2019, it had "45,000 customers located in over 100 countries," with a "total addressable market ("TAM") . . . greater than $10 billion."[15]

25. In the ordinary course of doing business with Defendant's clients, individuals are regularly required to provide Defendant's clients with sensitive, personal, and private information that is then stored, maintained, and secured by Defendant. This Private Information includes or may include the following personal data:

- Name;
- Address;
- Phone number(s);
- Email address;
- Date of birth;
- Demographic information;
- Social Security number;
- Credit card account numbers;
- Bank account numbers;

[12] *Id.*
[13] *Id.* at 7, 8.
[14] *Supra* note 10.
[15] 2019 Form 10-K at 3.

- Educational history;
- Healthcare records or other Health Information Portability and Accountability Act ("HIPAA") protected data;
- Insurance information and coverage;
- Photo identification;
- Employer information;
- Income information;
- Donor contribution information; and
- Place of birth, mother's maiden names, passwords, or other Private Information.

26. At all relevant times, Defendant knew the data it stores was vulnerable to cyber-attack. In its 2019 Annual Report, filed with the SEC in February 2020, Defendant specifically admitted its known susceptibility to cyberattacks. Specifically, Defendant states:

> 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.
>
> Fundamental to the use of our solutions is the secure collection, storage and transmission of confidential donor and end user data and transaction data, including in our payment services. Despite the network and application security, internal control measures, and physical security procedures we employ to safeguard our systems, we may still be vulnerable to a security breach, intrusion, loss or theft of confidential donor data and transaction data, which may harm our business, reputation and future financial results.[16]

27. Further, Defendant acknowledged the sophistication of attacks and the need to constantly evaluate and adjust its procedures:

[16] 2019 Form 10-K at 20.

> Like many major businesses, we are, from time to time, a target of cyber-attacks and phishing schemes, and we expect these threats to continue. Because of the numerous and evolving cybersecurity threats, including advanced and persistent cyber-attacks, phishing and social engineering schemes, used to obtain unauthorized access, disable or degrade systems have become increasingly more complex and sophisticated and may be difficult to detect for periods of time, we may not anticipate these acts or respond adequately or timely. As these threats continue to evolve and increase, we may be required to devote significant additional resources in order to modify and enhance our security controls and to identify and remediate any security vulnerabilities.[17]

28. As such, Defendant identified the risk of failing to detect an attack and the consequences of such a failure, including failure to respond adequately or on a timely basis. Additionally, Defendant identified the imminent risk inherent in a data breach and the duties a breach would trigger.

> A compromise of our data security that results in customer or donor personal or payment card data being obtained by unauthorized persons could adversely affect our reputation with our customers and others, as well as our operations, results of operations, financial condition and liquidity and could result in litigation against us or the imposition of penalties. We might be required to expend significant capital and other resources to further protect against security breaches or to rectify problems caused by any security breach, including notification under data privacy laws and regulations and expenses related to remediating our information security systems. Even though we carry cyber-technology insurance policies that may provide insurance coverage under certain circumstances, we might suffer losses as a result of a security breach that exceed the coverage available under our insurance policies or for which we do not have coverage. A security breach and any efforts we make to address such breach could also result in a disruption of our operations, particularly our online sales operations.[18]

29. Although Defendant identified these risks as its own, it demonstrates an acute awareness of the adverse effects that could result from a data breach, and, as such, apply to Plaintiff and Class Members.

> Further, the existence of vulnerabilities, even if they do not result in a security breach, may harm client confidence and require substantial resources to address, and we may not be able to discover or remedy such security vulnerabilities before they are exploited, which may harm our business, reputation and future financial results.[19]

---

[17] *Id.*
[18] *Id.*
[19] *Id.*

30. Because of the highly sensitive and personal nature of the Private Information Defendant maintains, manages, and secures with respect to the "end users" of its clients, like that of the Plaintiff here, Defendant has publicly affirmed its obligation and duty to secure Plaintiff's data.

31. Defendant's Privacy Policy North America ("Privacy Policy") expressly states:

> At Blackbaud, we are committed to protecting your privacy. This [Privacy] Policy applies to Blackbaud's collection and use of personal data in connection with our marketing and provision of the Blackbaud Solutions, customer support and other services (collectively, the "Services"), for example if you are a customer, visit the website, interact with us at industry conferences, or work for a current or prospective customer of the Services.[20]

32. Defendant represents with regard to the security of Personal Information:

> We restrict access to personal information collected about you at our website to our employees, our affiliates' employees, those who are otherwise specified in this [Privacy] Policy or others who need to know that information to provide the Services to you or in the course of conducting our business operations or activities. While no website can guarantee exhaustive security, we maintain appropriate physical, electronic and procedural safeguards to protect your personal information collected via the website. We protect our databases with various physical, technical and procedural measures and we restrict access to your information by unauthorized persons. We also advise all Blackbaud employees about their responsibility to protect customer data and we provide them with appropriate guidelines for adhering to our company's business ethics standards and confidentiality policies. Inside Blackbaud, data is stored in password-controlled servers with limited access.[21]

33. Defendant professes that its Privacy Policy is somehow supplanted by its clients:

> If you're a constituent, supporter, patient or student of one of our customers, to which we provide the Services, your data will be used in accordance with that customer's privacy policy. In providing the Services, Blackbaud acts as a service provider and thus, this [Privacy] Policy will not apply to constituents of our customers.[22]

---

[20] Blackbaud, Inc., *Privacy Policy North America*, https://www.blackbaud.com/company/privacy-policy/north-america (last visited Jan. 11, 2021).
[21] *Id.*
[22] *Id.*

34. Defendant cannot absolve itself from its obligation or duty based on assertion of a lack of privity, simply by arguing, as it did in a recent SEC filing, for example, that "plaintiffs lack contractual privity with us."[23]

35. The duty to protect Plaintiff's Private Information is non-delegable, particularly here where Defendant's entire business model is premised upon voluntarily assuming the duty via soliciting customers to utilize its professed ability to manage, house and safeguard data. Plaintiff alleges that under any privacy policy, Defendant is liable for the removal of this data.

36. Given the magnitude of the risk and repercussions of a breach or attack targeting this type of data, the likelihood of a breach or attack, and Defendant's explicit awareness of these vulnerabilities, Defendant should have taken every precaution in protecting Plaintiff's and Class Members' Private Information, or at least employed "appropriate" safeguards as it pledged in its Privacy Policy. However, Defendant failed to employ adequate safeguards, leaving the sensitive Private Information in its possession exposed to unauthorized access. This is especially concerning since Defendant serves many K-12 school providers, which ultimately placed minors' data at risk of unauthorized exposure and misuse.

37. In fact, the Private Information of children is particularly attractive to data thieves and can have long-lasting effects on the child's financial history and identity. Specifically,

> theft of a child's identity is lucrative to a cyber-criminal because it can remain undetected for years, if not decades. Without regular monitoring, a child's identity that has been stolen may not be discovered until they are preparing to go to college and start applying for student loans or get their first credit card. By then, the damage is done and the now young adult will need to go through the pain of proving that their identity was indeed stolen.[24]

---

[23] Blackbaud, Inc., Form 10-Q at 20 (Nov. 3, 2020), https://investor.blackbaud.com/static-files/b861e404-fa85-4f5b-a833-bc30de0165dd.

[24] Axiom Cyber Solutions, *How Data Breaches Affect Children* (Mar. 15, 2018), https://axiomcyber.com/data-breach/how-data-breaches-affect-children/.

38. In 2011, Carnegie Mellon University's CyLab reported "the rate of child identity theft is 51 times higher than for adults (whose data sets cost about $10 - $25 on dark web markets)."[25]

39. By early 2018, it became well known that the data of infants was being sold on the dark web. As of 2018, the cost of an infant's data was approximately $300 of bitcoin, which would "provide cybercriminals access to a clean credit history."[26]

40. As instructed by the Federal Trade Commission ("FTC"), "[a] child's Social Security number can be used by identity thieves to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live."[27]

41. As one cyber security author further explained, the impact of the use of children's information is further exacerbated by the fact that there are few checks on using a child's data to initially obtain credit and slowly increase it over time—all while being undetected by the child and the parents.[28] Thus, "[t]he problem goes unnoticed for years—possibly decades—before the child goes to apply for student loans, open their first credit card, or buy their first car."[29]

42. In fact, Defendant even committed to adopt enhanced safeguards for the maintenance of student's Private Information, a promise it has utterly failed to uphold. In April of 2015, Defendant signed a pledge to respect student data privacy and to safeguard student

---

[25] Selena Larson, *Infant Social Security Numbers Are for Sale on the Dark Web*, CNN Business (Jan. 22, 2018), https://money.cnn.com/2018/01/22/technology/infant-data-dark-web-identity-theft/index.html.
[26] *Id.*
[27] FTC, *Child Identity Theft*, https://www.consumer.ftc.gov/articles/0040-child-identity-theft (last visited Jan. 12, 2021).
[28] Emily Wilson, *The Worrying Trend of Children's Data Being Sold on the Dark Web*, TNW (Feb. 23, 2019), https://thenextweb.com/contributors/2019/02/23/children-data-sold-the-dark-web/.
[29] *Id.*

information for data obtained from all of its K-12 school provider clients. The Student Privacy Pledge, developed by the Future of Privacy Forum ("FPF") and the Software & Information Industry Association ("SIIA"), was created to "safeguard student privacy in the collection, maintenance and use of personal information."[30]

43. In signing the Student Privacy Pledge, Defendant specifically represented to students and parents of its K-12 school providers that it would, *inter alia*, "[m]aintain a comprehensive security program" and "[b]e transparent about collection and use of student data."[31]

44. In further support of this representation and promise to student and parent users, Travis Warrant, president of Defendant's K-12 Private Schools Group, stated:

> "Blackbaud is committed to protecting sensitive student data and security[.] The Pledge will better inform our customers, service providers and the general public of our dedication to protecting student privacy." The Pledge details ongoing industry practices that meet (and in some cases, exceed) all federal requirements, and encourages service providers to more clearly articulate their data privacy practices.[32]

45. Despite its duties, representations, and promises, Defendant failed to adequately secure and protect numerous K-12 providers, including St. Andrew's Episcopal School which maintained Plaintiff's and thousands of other students' Private Information, by allowing the Private Information to be accessed, copied, and potentially used or sold at a later date.

46. Further, due to HIPAA, Defendant had additional obligations to secure patient users' information for healthcare clients.

---

[30] Nicole McGougan, *Blackbaud Signs Pledge to Respect Student Data Privacy*, Blackbaud Inc. (Apr. 22, 2015), https://www.blackbaud.com/home/2015/04/22/blackbaud-signs-pledge-to-respect-student-data-privacy.
[31] *Id.*
[32] *Id.*

47. Defendant has further failed Plaintiff and Class Members by failing to adequately secure and protect their Private Information, by allowing the Private Information to be copied and potentially used or sold at a later date.

48. Defendant further failed Plaintiff and Class Members by failing to adequately notify them of the ransomware attack and resulting Data Breach or provide any remedy other than belated and facially inadequate notice.

THE DATA BREACH

49. Prior to the ransomware attack and Data Breach, Plaintiff and Class Members provided sensitive and personally-identifying Private Information to Defendant as part of, *inter alia*, seeking healthcare from healthcare providers; making donations to non-profit companies; seeking education from K-12 school providers and universities; or in seeking other services from Defendant's clients. When providing such information, these individuals had the expectation that Defendant, as the manager and securer of this Private Information, would maintain security against cybercriminals and cyberattacks.

50. Defendant maintained Plaintiff's and Class Members' data on a shared network, server, and/or software. Despite its own awareness of steady increases of cyberattacks on health care providers, schools, and other facilities over the course of recent years, Defendant did not maintain adequate security of Plaintiff's and Class Members' data, or adequately protect it against hackers and cyberattacks.

51. According to its own statements, posted to its website in July 2020, Defendant initially discovered a ransomware attack in May of 2020.[33] The attack attempted to "disrupt the

[33] *Supra* note 7.

business by locking companies out of their own data and servers."[34] According to Defendant's statements:

> After discovering the attack, our Cyber Security team—together with independent forensics experts and law enforcement—successfully prevented the cybercriminal from blocking our system access and fully encrypting files; and ultimately expelled them from our system. Prior to our locking the cybercriminal out, the cybercriminal removed a copy of a subset of data from our self-hosted environment. **The cybercriminal did not access credit card information, bank account information, or social security numbers.** 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. Based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have no reason to believe that any data went beyond the cybercriminal, was or will be misused; or will be disseminated or otherwise made available publicly. . . . The subset of customers who were part of this incident have been notified and supplied with additional information and resources. We apologize that this happened and will continue to do our very best to supply help and support as we and our customers jointly navigate this cybercrime incident.[35]

52. The ransomware attack that began in February of 2020 and continued until May of 2020 led to the removal of one or more copies of a subset of the accessed data.

53. Although Defendant claims that credit card information or bank account information was not accessed, the Notice Plaintiff received from St. Andrew's Episcopal School advises individuals whose Private Information was accessed to, *inter alia*, follow "recommendations by the [FTC] regarding identity theft protection" to include "plac[ing] a fraud alert or security freeze on your credit file."[36] Defendant's statements of reassurance were unfounded in light of their earlier admission to the SEC: "further forensic investigation found that for some of the notified customers, the cybercriminal may have accessed some unencrypted fields

[34] *Id.*
[35] Blackbaud, Inc., *Security Incident* (July 19, 2020), https://www.blackbaud.com/securityincident [https://web.archive.org/web/20200719013019/https://www.blackbaud.com/securityincident] (emphasis added). Notably the language in bold has since been removed.
[36] Ex. A at 2.

intended for bank account information, [S]ocial [S]ecurity numbers, usernames and/or passwords."[37]

54. Defendant did not have a sufficient process or policies in place to prevent cyberattack and access, which is evident by its own statements that it has "already implemented changes to prevent this specific issue from happening again."[38]

55. The acknowledged types of data exposed included Plaintiff's Private Information, such as Plaintiff's and Class Members' name, address, phone number(s), email address, date of birth, and/or Social Security number.[39]

56. Defendant should not be allowed to reasonably rely on the word of cyber criminals that the "copied" or stolen subset of any data was destroyed. Defendant has not and cannot be assured that Social Security numbers, bank account numbers, and credit card numbers were not also accessed and retained by the data thieves, or it would not have advised its clients to advise affected individuals to monitor accounts for suspicious activity. Despite recognizing the need for ongoing monitoring due to significant heightened risk, Defendant offered only a scant 24 months of credit monitoring, limited to only one of three reporting service, and provides little support and no remuneration in the event of an actual identity theft or misuse

57. Despite having knowledge of the attack and compromised stolen data since at least May 2020, Defendant willfully and knowingly withheld this knowledge from its affected clients and their constituents who were victims of the fraud until mid-July or August 2020.

58. Defendant has obligations and duties created by state and federal law, contracts, industry standards, common law, and representations made to the clients who entrusted Plaintiff's

[37] *Supra* note 4 at 2.
[38] *Supra* note 7.
[39] Ex. A at 1.

and others' data to Defendant's care to keep Private Information secure, confidential, and protected from unauthorized access and disclosure.

59. Indeed, cyberattacks have become so notorious that as recently as November 2019, the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issued warnings to potential targets like Defendant so they are aware of, and prepared for, a potential attack.[40]

60. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including by Defendant's own admissions in its 2019 Annual Report.[41]

61. Defendant breached its obligations to Plaintiff and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard Defendant's computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect consumers' Private Information;

c. Failing to properly monitor their own data security systems for existing intrusions;

d. Failing to timely notify its Clients, Plaintiff, and Class Members of the data breach; and

e. In other such ways yet to be discovered.

[40] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (emphasis added).
[41] 2019 Form 10-K at 20.

62. As the result of Defendant's failure to take certain measures to prevent the attack before it occurred, Defendant negligently and unlawfully failed to safeguard Plaintiff's Private Information.

63. Accordingly, as outlined below, Plaintiff's daily life was disrupted and Plaintiff and Class Members face an increased risk of fraud and identity theft.

CYBERATTACKS AND DATA BREACHES CAUSE DISRUPTION AND PUT CONSUMERS AT AN INCREASED RISK OF FRAUD AND IDENTIFY THEFT

64. Cyberattacks and data breaches of medical facilities, schools, and non-profit entities are especially problematic because of the disruption they cause to the overall daily lives of individuals affected by the attack.

65. Perhaps most illustrative of the danger that can be caused by cyberattacks on medical facilities, the first known death from a cyberattack was recently reported in Germany after a ransomware attack crippled a hospital's systems and they were forced to turn away emergency patients.[42]

66. The U.S. Government Accountability Office ("GAO") released a report in 2007 regarding data breaches finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[43]

67. The FTC recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if

---

[42] Melissa Eddy & Nicole Periroth, *Cyber Attack Suspected in German Woman's Death*, N.Y. Times (Sept. 18, 2020), https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

[43] U.S. Gov't Accountability Off., GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2 (June 2007), https://www.gao.gov/assets/270/262899.pdf.

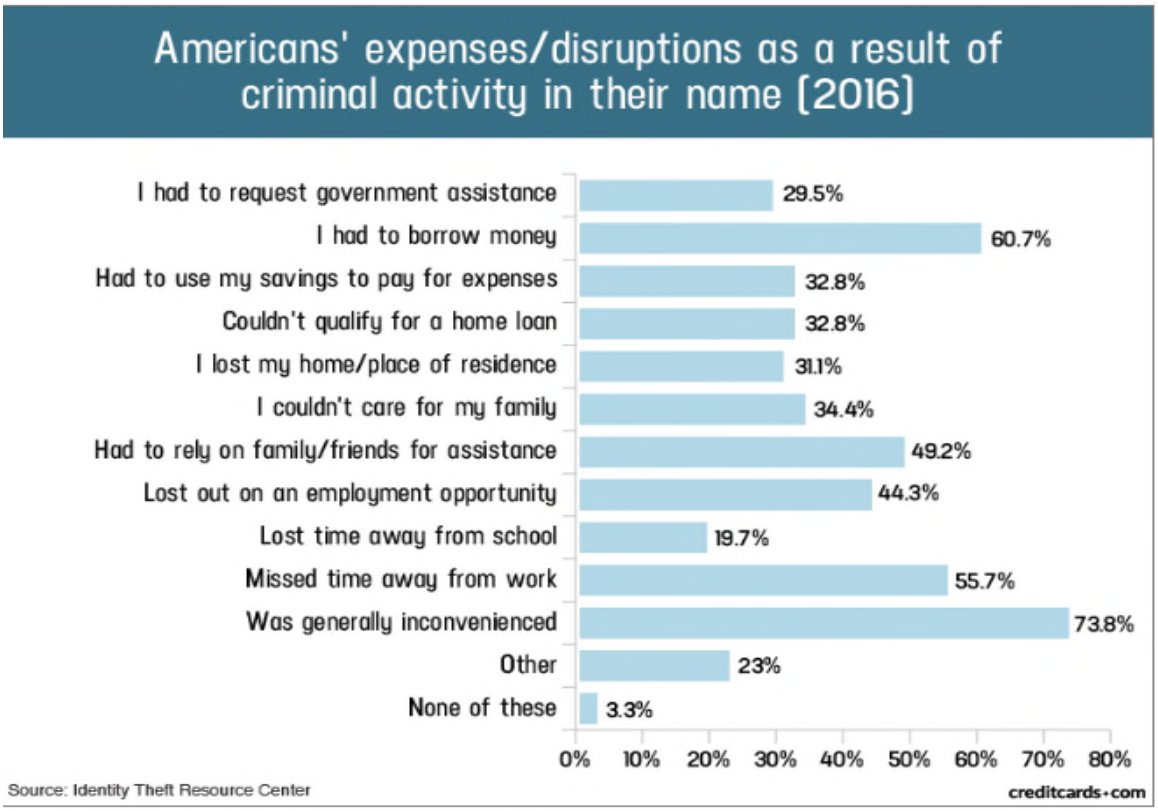
identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[44]

68. Cyber criminals use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

69. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name, but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, seek unemployment or other benefits, and may even give the victim's Private Information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[45]

[44] FTC, *Identity Theft Recovery Steps*, https://www.identitytheft.gov/Steps (last visited Jan. 12, 2021).

[45] Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (updated Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php [https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php] (last visited Jan. 12, 2021).



70. Private Information is a valuable property right.[46] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. This obvious risk to reward analysis illustrates that Private Information have considerable market value that is diminished when it is compromised.

71. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen

[46] *See, e.g.*, John T. Soma et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *1 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.")

> data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[47]

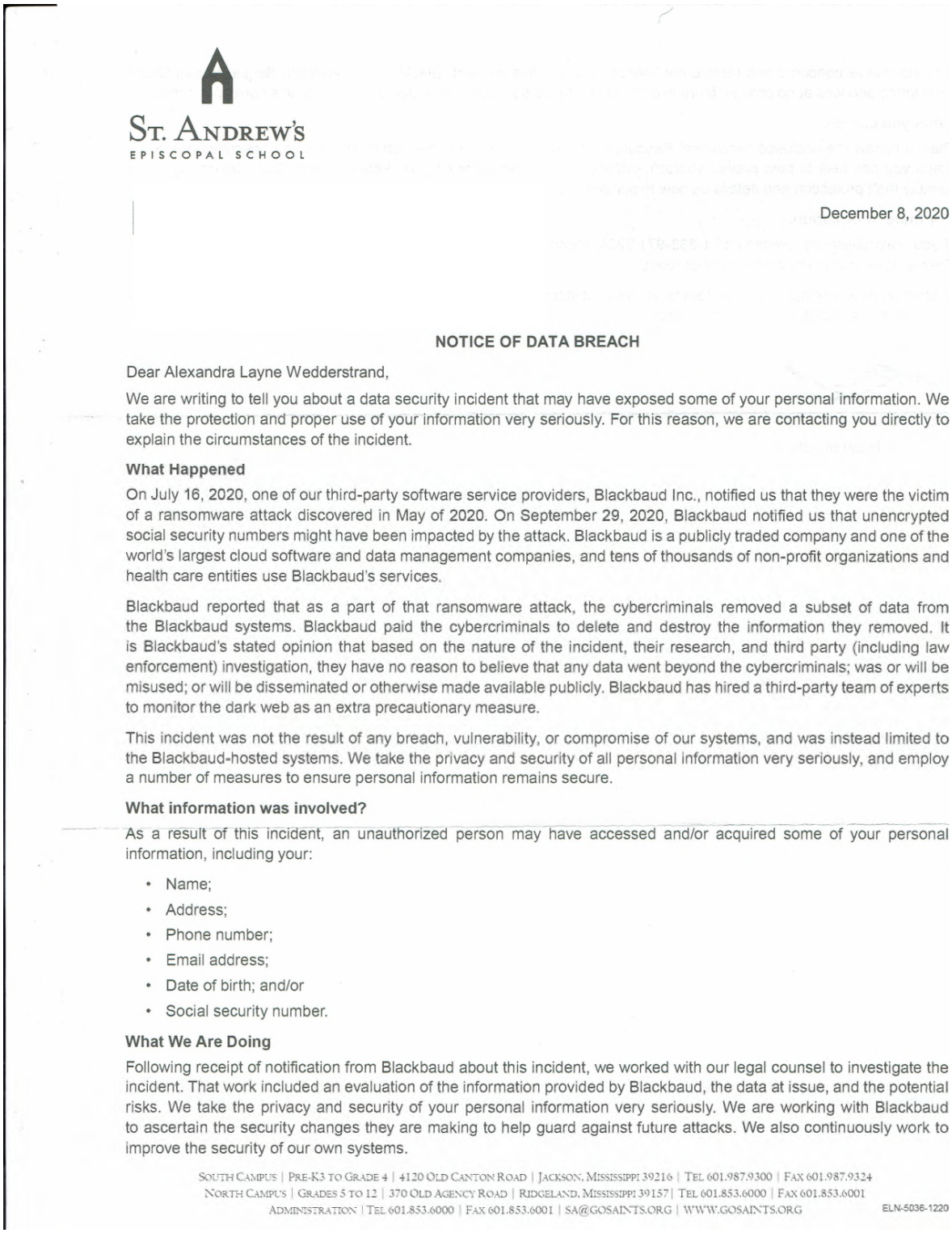
Private Information is such an inherently valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the cyber black-market for years.

72. There is a strong probability that entire batches of stolen information have yet to be dumped on the black market, meaning Plaintiff is at an increased risk of fraud and identity theft for many years into the future. Thus, as the Notice advises, Plaintiff must vigilantly monitor her financial accounts for many years to come.[48]

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

73. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach. The Private Information of Plaintiff Mitchell was compromised as a direct and proximate result of the Data Breach. While the compromise of this information was known as early as May of 2020, Plaintiff Mitchell did not receive Notice until December 8, 2020.[49]

[47] GAO Report at 28-29.
[48] *See* Ex. A.
[49] *Id.*



ST. ANDREW'S
EPISCOPAL SCHOOL

December 8, 2020

NOTICE OF DATA BREACH

Dear Alexandra Layne Wedderstrand,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What Happened

On July 16, 2020, one of our third-party software service providers, Blackbaud Inc., notified us that they were the victim of a ransomware attack discovered in May of 2020. On September 29, 2020, Blackbaud notified us that unencrypted social security numbers might have been impacted by the attack. Blackbaud is a publicly traded company and one of the world's largest cloud software and data management companies, and tens of thousands of non-profit organizations and health care entities use Blackbaud's services.

Blackbaud reported that as a part of that ransomware attack, the cybercriminals removed a subset of data from the Blackbaud systems. Blackbaud paid the cybercriminals to delete and destroy the information they removed. It is Blackbaud's stated opinion that based on the nature of the incident, their research, and third party (including law enforcement) investigation, they have no reason to believe that any data went beyond the cybercriminals; was or will be misused; or will be disseminated or otherwise made available publicly. Blackbaud has hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

This incident was not the result of any breach, vulnerability, or compromise of our systems, and was instead limited to the Blackbaud-hosted systems. We take the privacy and security of all personal information very seriously, and employ a number of measures to ensure personal information remains secure.

What information was involved?

As a result of this incident, an unauthorized person may have accessed and/or acquired some of your personal information, including your:

- Name;
- Address;
- Phone number;
- Email address;
- Date of birth; and/or
- Social security number.

What We Are Doing

Following receipt of notification from Blackbaud about this incident, we worked with our legal counsel to investigate the incident. That work included an evaluation of the information provided by Blackbaud, the data at issue, and the potential risks. We take the privacy and security of your personal information very seriously. We are working with Blackbaud to ascertain the security changes they are making to help guard against future attacks. We also continuously work to improve the security of our own systems.

SOUTH CAMPUS | PRE-K3 TO GRADE 4 | 4120 OLD CANTON ROAD | JACKSON, MISSISSIPPI 39216 | TEL 601.987.9300 | FAX 601.987.9324
NORTH CAMPUS | GRADES 5 TO 12 | 370 OLD AGENCY ROAD | RIDGELAND, MISSISSIPPI 39157 | TEL 601.853.6000 | FAX 601.853.6001
ADMINISTRATION | TEL 601.853.6000 | FAX 601.853.6001 | SA@GOSAINTS.ORG | WWW.GOSAINTS.ORG

ELN-5036-1220

74. Specifically, Plaintiff Mitchell, now a full-time graduate student, attended St. Andrew's Episcopal School, a client of Defendant, from 2001 through her high school graduation

in 2014. As a student at this school, Plaintiff was required to provide Private Information to St. Andrew's Episcopal School, which, in turn, relied upon Defendant to "secure" and maintain this Private Information. Included in the compromised Private Information were name, date of birth, and Social Security number.

75. Consequently, and given Plaintiff's young age, even if she used credit monitoring, data thieves could conceivably wait another seven or more years to sell or use her Private Information without detection. Thus, Plaintiff will require more than the average seven years of credit monitoring to ensure that her identity will be secure in the wake of this massive Data Breach.

76. To date, Defendant has provided Plaintiff with "Single Credit Bureau Monitoring," which provides data access to only one of the three national credit reporting bureaus, and only for a period of 24 months, while the threat to Plaintiff's credit or identity will continue for decades. Beyond this two-year window, Defendant offers no assistance or protection, even if identity theft occurs thereafter.

77. Further, even if Plaintiff's credit is frozen, she will eventually need to unfreeze her credit in order to obtain a car loan, obtain a mortgage, apply for jobs and various other tasks associated with building and strengthening her credit and transitioning into adult life. Doing so will make her vulnerable again in the future.

78. Like Plaintiff, other Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

79. As a direct and proximate result of Defendant's conduct, Plaintiff has been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

80. As a direct and proximate result of Defendant's conduct, Plaintiff has been forced to expend time dealing with the effects of the Data Breach. For example, Plaintiff is in the process

of exploring how to obtain a new Social Security number, which is a cumbersome and time-consuming process.

81. Plaintiff faces substantial risk of out-of-pocket fraud losses such as loans opened in her name, medical services billed in her name, tax return fraud, utility bills opened in her name, credit card fraud, and similar identity theft.

82. Plaintiff faces substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on her Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff.

83. Plaintiff will incur out-of-pocket costs for protective measures such as on-going credit monitoring fees, and may also incur additional costs for credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

84. Plaintiff also suffered a loss of value of her Private Information when it was removed and acquired by cyber thieves in the Data Breach.

85. Plaintiff has spent and will continue to spend significant amounts of time to respond to the Data Breach and monitor her financial, student, and/or medical accounts and records for misuse.

86. Plaintiff has suffered or will suffer actual injury as a direct result of the Data Breach. Plaintiff has and will suffer ascertainable losses in the form of out-of-pocket expenses and/or the loss of the value of her time spent in reasonably acting to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing her inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Placing "freezes" and "alerts" with credit reporting agencies;

f. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

g. Contacting financial institutions and closing or modifying financial accounts;

h. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled;

j. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come; and

k. Interacting with government agencies and law enforcement to address the impact and harm caused by this breach.

87. Moreover, Plaintiff has an interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing her data is not accessible online and that access to such data is limited and secured.

88. As a result of Defendant's failures to safeguard Plaintiff's data, Plaintiff is forced to live with the knowledge that her Private Information—which contains private and personal details of her life—may be disclosed to the entire world, thereby making her vulnerable to cyber criminals, permanently subjecting her to loss of security, and depriving her of her fundamental right to privacy.

89. As many of the purchasers of Private Information may not utilize the stolen information immediately, Plaintiff will be forced for long periods of time to endure the fear of whether and how such information will be used against her.

90. As a direct and proximate result of Defendant's actions and inactions, Plaintiff has suffered anxiety, emotional distress, and loss of privacy, and is at an increased risk of harm.

CLASS ACTION ALLEGATIONS

91. Plaintiff Mitchell brings this action on her own behalf and on behalf of all natural persons similarly situated.

92. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> Nationwide Class: All natural persons residing in the United States whose Personally Identifiable Information (PII) or Private Health Information (PHI) was compromised as a result of the Blackbaud data breach.

93. Plaintiff also proposes the following Subclass definitions, subject to amendment as appropriate:

> Colorado Subclass: All natural persons residing in Colorado whose Personally Identifiable Information (PII) or Private Health Information (PHI) was compromised as a result of the Blackbaud data breach.

94. Excluded from the Class and Subclass are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class and Subclass are members of the judiciary to whom this case is assigned, their families and members of their staff.

95. Numerosity. The members of the Class (and Subclass) are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff

at this time, based on information and belief, the Class consists of approximately hundreds of thousands of persons and entities whose data was compromised in the Data Breach.

96. Commonality. There are questions of law and fact common to Plaintiff and the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant truthfully represented the nature of its security systems, including their vulnerability to hackers;

d. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

e. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

f. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

g. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

h. Whether computer hackers obtained, sold, copied, stored or released Class Members' Private Information;

i. Whether Defendant knew or should have known that their data security systems and monitoring processes were deficient;

j. Whether Plaintiff suffered legally cognizable damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant's conduct was *per se* negligent;

m. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

n. Whether Defendant failed to provide accurate and complete notice of the Data Breach in a timely manner; and

o. Whether Plaintiff is entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

97. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

98. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

99. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and Class Members' data at issue here was stored on the same computer systems and allowed to be unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members, as described *supra*, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

100. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for Defendant. In

contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each class member.

101. Defendant has acted on grounds that apply generally to the Class (and Subclass) as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

FOR A FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff, the Nationwide Class, and Colorado Subclass Members)

102. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 101 above, as if fully set forth herein.

103. Defendant's clients required Plaintiff and Class Members to submit non-public personal information in order to obtain medical, educational, and other services. Defendant had a duty to Class Members to securely maintain the Private Information collected as promised and warranted.

104. By voluntarily accepting the duty to maintain and secure this data, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer systems—and Plaintiff's Private Information held within it—to prevent disclosure of the information, and to safeguard the information from cyber theft. Defendant's duty included a responsibility to implement systems and processes by which it could detect and prevent a breach of its security systems in an expeditious manner and to give prompt notice to those affected by a data breach and/or ransomware attack.

105. Defendant owed a duty of care to Plaintiff to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and

networks, and the personnel responsible for them, adequately protected and safeguarded the Private Information of the Class.

106. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Class Members, the end users of the services Defendants provided to its clients, which is recognized by Defendant's Privacy Policy, as well as applicable laws and regulations. Defendant actively solicited Private Information as part of its business and was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a ransomware attack and resulting data breach.

107. Defendant had a specific duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

108. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

109. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' data. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

f. Failing to timely notify Class Members about the Data Brach so those put at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages.

110. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of ransomware attacks and data breaches.

111. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

112. Plaintiff is entitled to compensatory and consequential damages suffered as a result of the Data Breach.

113. Plaintiff is also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide robust and adequate credit monitoring to all Class Members, and any other relief this count deems just and proper.

FOR A SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff, the Nationwide Class, and Colorado Subclass Members)

114. Plaintiff re-alleges and incorporate by reference Paragraphs 1 through 113 above, as if fully set forth herein.

115. When Plaintiff and Class Members provided their Private Information to Defendant and Defendant's clients in exchange for Defendant and Defendant's clients' services, they entered

into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

116. Defendant solicited and invited Class Members to provide their Personal Information as part of Defendant's regular business practices, including through its Privacy Policy. Plaintiff and Class Members accepted Defendant's offers and provided their data to Defendant.

117. In entering into such implied contracts, Plaintiff reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

118. Plaintiff accepted service from, and paid money to Defendant's clients which was conferred upon Defendant, and through which Plaintiff reasonably believed and expected that Defendant would use part of those funds to maintain adequate data security. Defendant failed to do so.

119. Plaintiff would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep that information secure. Plaintiff would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

120. Plaintiff fully and adequately performed her obligations under the implied contracts with Defendant.

121. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their data.

122. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

123. Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

124. Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FOR A THIRD CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff, the Nationwide Class, and Colorado Subclass Members)

125. Plaintiff re-alleges and incorporate by reference Paragraphs 1 through 124, above as if fully set forth herein.

126. Pursuant to the FTCA, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

127. Pursuant to the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801, Defendant had a duty to protect the security and confidentiality of Plaintiff's and Class Members' Private Information.

128. Defendant breached its duties to Plaintiff and Class Members under the FTCA and the GLBA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

129. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

130. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' data would not have been stolen and they would not have been harmed.

131. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information, including increased risk of identity theft.

132. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FOR A FOURTH CAUSE OF ACTION
VIOLATION OF THE COLORADO SECURITY BREACH NOTIFICATION ACT,
Colo. Rev. Stat. §§ 6-1-716, *et seq.*
(On Behalf of Plaintiff and Colorado Subclass Members)

133. Plaintiff Mitchell, individually and on behalf of Colorado Subclass members, re-alleges and incorporates by reference Paragraphs 1 through 132 above, as if fully set forth herein.

134. Plaintiff Mitchell and Colorado Subclass members' Private Information (e.g., Social Security numbers) includes "Personal Information" as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

135. Defendant is a business that owns or licenses computerized data that includes "Personal Information" as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

136. Defendant is required to accurately notify Plaintiff and Colorado Subclass members if it becomes aware of a breach of its data security system in the most expedient time possible without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

137. Because Defendant was aware of a breach of its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

138. By failing to disclose the Data Breach in a timely and accurate manner, Defendant violated Colo. Rev. Stat. § 6-1-716(2).

139. As a direct and proximate result of Defendant's violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff and Colorado Subclass members suffered damages, as described above.

140. Plaintiff Mitchell and the Colorado Subclass members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

FOR A FIFTH CAUSE OF ACTION
VIOLATION OF THE COLORADO CONSUMER PROTECTION ACT,
Colo Rev. Stat. §§ 6-1-101, *et seq.*
(On Behalf of Plaintiff and Colorado Subclass Members)

141. Plaintiff Mitchell, individually and on behalf of Colorado Subclass members, re-alleges and incorporates by reference Paragraphs 1 through 140 above, as if fully set forth herein.

142. Defendant is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

143. Defendant engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

144. Plaintiff and Colorado Subclass members, as well as the general public, are actual or potential consumers of the products and services offered by Defendant or successors in interest to actual consumers.

145. Defendant engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

a. Knowingly making a false representation as to the characteristics of products and services; and

b. Representing that services are of a particular standard, quality, or grade, though Defendant knew or should have known that they were otherwise.

146. Defendant's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Colorado Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Private Information, including duties imposed by the FTCA, 15 U.S.C.§ 45, the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Colorado Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Colorado Subclass members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Private Information, including duties imposed by the FTCA, 15 U.S.C.§ 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

147. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

148. Defendant intended to mislead Plaintiff and Colorado Subclass members and induce them to rely on its misrepresentations and omissions.

149. Had Defendant disclosed to Plaintiff and Colorado Subclass members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant was trusted with sensitive and valuable Private Information regarding hundreds of thousands of consumers, including Plaintiff and the Colorado Subclass. Defendant accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Defendant held itself out as maintaining a secure platform for Private Information data, Plaintiff and the Colorado Subclass members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

150. Defendant acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff and Colorado Subclass members' rights.

151. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Colorado Subclass members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their Private Information.

152. Plaintiff and Colorado Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b) $500, or (c) three times actual damages (for Defendant's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members or to mitigate further harm;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than seven years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including reasonable expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMAND

Plaintiff hereby demands a jury trial for all claims so triable.

Dated this 14th of January, 2021

Respectfully submitted,

KELLER ROHRBACK L.L.P.

/s/ Gretchen Freeman Cappio
Gretchen Freeman Cappio (*pro hac vice forthcoming*)
Juli E. Farris (*pro hac vice forthcoming*)
Cari Campen Laufenberg (*pro hac vice forthcoming*)
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Tel.: (206) 623-1900
Fax: (206) 623-3384
Email: gcappio@kellerrohrback.com
jfarris@kellerrohrback.com
claufenberg@kellerrohrback.com

Alison E. Chase (*pro hac vice forthcoming*)
KELLER ROHRBACK L.L.P.
801 Garden St., Suite 301

Santa Barbara, CA 93101
Tel.: (805) 456-1962
Fax: (206) 456-1497
Email: achase@kellerrohrback.com

/s/ Marlon E. Kimpson
Marlon E. Kimpson (SC Bar No. 17042)
Jodi Westbrook Flowers (SC Bar No. 066300)
Mathew Jasinski (*pro hac vice forthcoming*)
Andrew P. Arnold (SC Bar No. 102491)
Tammy C. Rivers (SC Bar No. 102812)
C. Ross Heyl (SC Bar No. 104154)
MOTLEY RICE LLC
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Tel.: (843)216-9000
Fax: (843)216-9027
Email: mkimpson@motleyrice.com
jflowers@motleyrice.com
mjasinski@motleyrice.com
aarnold@motleyrice.com
rheyl@motleyrice.com
tcrivers@motleyrice.com

Attorneys for Plaintiff and the Proposed Class

ST. ANDREW'S
EPISCOPAL SCHOOL

[redacted]

December 8, 2020

NOTICE OF DATA BREACH

Dear Alexandra Layne Wedderstrand,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What Happened

On July 16, 2020, one of our third-party software service providers, Blackbaud Inc., notified us that they were the victim of a ransomware attack discovered in May of 2020. On September 29, 2020, Blackbaud notified us that unencrypted social security numbers might have been impacted by the attack. Blackbaud is a publicly traded company and one of the world's largest cloud software and data management companies, and tens of thousands of non-profit organizations and health care entities use Blackbaud's services.

Blackbaud reported that as a part of that ransomware attack, the cybercriminals removed a subset of data from the Blackbaud systems. Blackbaud paid the cybercriminals to delete and destroy the information they removed. It is Blackbaud's stated opinion that based on the nature of the incident, their research, and third party (including law enforcement) investigation, they have no reason to believe that any data went beyond the cybercriminals; was or will be misused; or will be disseminated or otherwise made available publicly. Blackbaud has hired a third-party team of experts to monitor the dark web as an extra precautionary measure.

This incident was not the result of any breach, vulnerability, or compromise of our systems, and was instead limited to the Blackbaud-hosted systems. We take the privacy and security of all personal information very seriously, and employ a number of measures to ensure personal information remains secure.

What information was involved?

As a result of this incident, an unauthorized person may have accessed and/or acquired some of your personal information, including your:

- Name;
- Address;
- Phone number;
- Email address;
- Date of birth; and/or
- Social security number.

What We Are Doing

Following receipt of notification from Blackbaud about this incident, we worked with our legal counsel to investigate the incident. That work included an evaluation of the information provided by Blackbaud, the data at issue, and the potential risks. We take the privacy and security of your personal information very seriously. We are working with Blackbaud to ascertain the security changes they are making to help guard against future attacks. We also continuously work to improve the security of our own systems.

To help relieve concerns and restore confidence following this incident, Blackbaud is providing Single Bureau Credit Monitoring services at no charge. More information on those services is provided at the end of this correspondence.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-833-971-3254, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Kevin Lewis
Associate Head of School

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 119016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Credit Monitoring

Blackbaud is providing you with access to Single Bureau Credit Monitoring services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

Proactive Fraud Assistance. For sensitive breaches focused on customer retention, reputation management, or escalation handling, CyberScout provides unlimited access during the service period to a fraud specialist who will work with enrolled notification recipients on a one-on-one basis, answering any questions or concerns that they may have. Proactive Fraud Assistance includes the following features:

- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Identity Theft and Fraud Resolution Services. Resolution services are provided for enrolled notification recipients who fall victim to an identity theft as a result of the applicable breach incident. ID Theft and Fraud Resolution includes, but is not limited to, the following features:

- Unlimited access during the service period to a personal fraud specialist via a toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes.
- All phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to any relevant government and private agencies.
- Assistance with filing a law enforcement report.
- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).
- Assistance with placement of credit file freezes in states where it is available and in situations where it is warranted (United States only); this is limited to online-based credit freeze assistance.
- Customer service support for individuals when enrolling in monitoring products, if applicable.
- Assistance with review of credit reports for possible fraudulent activity.
- Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Enrollment Instruction - How do I enroll for the free services?
To enroll in Credit Monitoring services at no charge, please navigate to:
https://www.cyberscouthq.com/epiq263?ac=263HQ1734

If prompted, please provide the following unique code to gain access to services:
263HQ1734

Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. **Please ensure you take this step to receive your alerts.**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.