UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

RICHARD KREFTING, individually and on behalf of all others similarly situated, Plaintiff, v. KAYE-SMITH ENTERPRISES, Inc., and BOEING EMPLOYEES' CREDIT UNION, Defendants.	No. 2:23-cv-00220 CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiff Richard Krefting ("Plaintiff"), individually and on behalf of all other similarly situated individuals, and by and through their undersigned counsel files this Class Action Complaint against Defendant Kaye-Smith Enterprises, Inc. ("Kaye-Smith"") and Defendant Boeing Employees' Credit Union ("BECU") (collectively "Defendants") and alleges the following based upon their personal knowledge of the facts, and upon information and belief based on the investigation of counsel as to all other matters.

NATURE OF THE ACTION

1. Kaye-Smith is a marketing execution and supply chain company, serving corporate clients across a wide range of industries, including providing statement processing and billing services, inventory management, direct mail marketing, web applications, warehousing and distribution, data management and personalized fulfillment. For business purposes, Kaye-Smith

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

receives the information of individuals from customer organizations which Defendant utilizes to conduct mailings on behalf of their customers.[1]

2. One of the corporate clients Kaye-Smith serves is BECU, a credit union that serves customers with banking services. As a condition of BECU and Kaye-Smith's relationship, BECU provided Plaintiff's and Class Members' personally identifiable information to Kaye-Smith. Kaye-Smith, in turn, stored that information on its' system.

3. Plaintiff and the Class Members (as further defined below) have had their personally identifiable information exposed as a result of Kaye-Smith's inadequately secured computer network. Kaye-Smith betrayed of its obligations to Plaintiff and the other Class Members by failing to properly safeguard and protect their personally identifiable information and thereby enabling cybercriminals to steal such valuable and sensitive information.

4. This class action seeks to redress Kaye-Smith's unlawful, willful and wanton failure to protect the personally identifiable information of hundreds of thousands of individuals that was exposed in a major data breach of Kaye-Smith's network (the "Data Breach" or "Breach"), in violation of its legal obligations.

5. The Data Breach was discovered in May 2022, when Kaye-Smith learned that a cyberattack had been successfully launched on its systems.[2] Kaye-Smith investigated the attack with the assistance of third-party computer specialists. The forensic investigation determined that cybercriminals gained unauthorized access to certain systems containing the personally identifiable information of hundreds of thousands of individuals.[3]

---

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/d60746ac-15bf-49ce-bc64-c15171874102.shtml*; see also* https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-574.pdf; *Smith v. Boeing Employees' Credit Union*, Case No. 2:22-cv-01234, ECF No. 10 at 1, n.2 (identifying Kaye-Smith as the vendor).
[2] *See* https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-574.pdf.
[3] *Id.*; *see also* https://apps.web.maine.gov/online/aeviewer/ME/40/d60746ac-15bf-49ce-bc64-c15171874102.shtml.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

6. According to Kaye-Smith and information provided by its affected customers, the personally identifiable information exposed in the Breach included: names, addresses, Social Security numbers, account numbers, credit score ("PII") and medical information ("PHI") (collectively "Private Information").[4]

7. It was negligent of BECU to provide Plaintiff's and Class Members' PII and financial information to a third-party who lacked adequate security systems.

8. Due to Defendants' negligence, cybercriminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of Plaintiff and the Class Members.

9. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Plaintiff and Class Members will have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, and/or additional damages as described below.

10. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

---

[4] *See* Plaintiff's breach notification letter, attached as Exhibit 1; *see also* https://www.hipaajournal.com/data-breaches-reported-by-allegheny-health-network-st-lukes-health-system-goldsboro-podiatry/.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

I. THE PARTIES

Plaintiff

11. Plaintiff Richard Krefting is domiciled in and a citizen of the state of Washington.

12. On or around July 25, 2022, Plaintiff received a breach notification letter from BECU informing him that his personal information, including name, address, account number(s), credit score, and Social Security number had been exposed to cybercriminals during the Data Breach.[5]

Defendant Kaye-Smith

13. Defendant Kaye-Smith is a marketing and supply chain corporation with its principal place of business in Portland, Oregon. Kaye-Smith conducts business out of Renton, Washington.

14. Kaye-Smith provides statement processing and billing services, inventory management, direct mail marketing, web applications, warehousing and distribution, and data management services for numerous companies across the United States. For business purposes, Kaye-Smith received the information of individuals from customer organizations which Kaye-Smith utilized to conduct these services on behalf of their customers.[6]

15. **Defendant BECU** Defendant BECU is a credit union with its principal place of business in Tukwila, Washington.

16. BECU provides baking services to customers.[7]

---

[5] Upon information and belief, Kaye-Smith is the "printing vendor" referenced in the BECU breach notification letter. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/d60746ac-15bf-49ce-bc64-c15171874102.shtml*; see also* https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-574.pdf; *Smith v. Boeing Employees' Credit Union*, Case No. 2:22-cv-01234, ECF No. 10 at 1, n.2 (identifying Kaye-Smith as the vendor).

[6] *See* https://kayesmith.com.

[7] [7] https://www.becu.org (last accessed October 19, 2022)

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

II. JURISDICTION AND VENUE

17. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendants.

18. This Court has personal jurisdiction over Defendants because they are headquartered in and/or operate within this District and regularly transact business, have agents, and are otherwise within this District. Venue is likewise proper as to Defendants in this District because many Class Members reside in this District, and a substantial part of the events or omissions giving rise to the claim occurred in this District. 28 U.S.C. § 1391(b)(2).

III. FACTUAL ALLEGATIONS

A. The Data Breach

19. Based on information supplied by Kaye-Smith, the Data Breach was discovered in May 2022, when Kaye-Smith learned that a cyberattack had been successfully launched on its systems.[8] Kaye-Smith investigated the attack with the assistance of third-party computer specialists. The forensic investigation determined that cybercriminals gained unauthorized access to certain systems containing the personally identifiable information of hundreds of thousands individuals.[9]

20. According to Kaye-Smith and information provided by its affected customers, the personally identifiable information exposed in the Breach included: names, addresses, Social Security numbers, account numbers, credit score, and medical information.[10]

---

[8] *See* https://www.mass.gov/doc/assigned-data-beach-number-28266-kaye-smith-enterprises-inc/download.
[9] *Id.*; *see also* https://apps.web.maine.gov/online/aeviewer/ME/40/d60746ac-15bf-49ce-bc64-c15171874102.shtml.
[10] *Id.*; *see also* Plaintiff's breach notification letter, attached as Exhibit 1.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

21. Kaye-Smith failed to take the necessary precautions required to safeguard and protect Plaintiff's and the other Class Members' Private Information from unauthorized disclosure. Kaye-Smith's actions represent a flagrant disregard of the rights of the Class Members, both as to privacy and property.

22. BECU failed to ensure Kaye-Smith had proper safeguards in place prior to sharing Plaintiff's and other Class Members' Private Information.

B. Plaintiff's Experiences

23. On or around July 25, 2022, Plaintiff received a breach notification letter from BECU informing him that his personal information, including name, address, account number(s), credit score, and Social Security number had been exposed to cybercriminals during the Data Breach. Upon information and belief, Kaye-Smith is the "printing vendor" referenced in the BECU breach notification letter.[11] The letter Plaintiff received is attached as Exhibit 1 hereto.

24. Plaintiff's and Class Members' Private Information was entrusted to BECU, and then to Kaye-Smith with the reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

25. Because of the Data Breach, Plaintiff's and Class Members' Private Information is now in the hands of cyber criminals. Plaintiff and all Class Members are now imminently at risk of crippling future identity theft and fraud.

26. Plaintiff has already experienced identity theft. Indeed, following the Data Breach, Plaintiff has discovered a credit account fraudulently opened using his personal information. Additionally, since the Data Breach, Plaintiff has received notifications from Credit Karma that

[11] This is supported, among other things, by the similar timing and information provided by Defendant.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

someone has attempted to change the location of his home address and that someone has made a credit inquiry without his permission.

27. As a result of the Data Breach, Plaintiff has already spent numerous hours responding to the Data Breach. Among other things, Plaintiff has spent time researching the facts and scope of the Data Breach, monitoring his accounts and personal information, reviewing his credit reports, responding to the fraudulent activity he is already experienced, and taking other steps in an attempt to mitigate the adverse consequences of the Data Breach.

28. As a direct and proximate result of the Data Breach, Plaintiff will likely need to purchase a lifetime subscription for identity theft protection and credit monitoring.

29. Plaintiff has been careful to protect and monitor his identity.

30. Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cybercriminals; (c) damages to and diminution in value of Plaintiff's Private Information that was entrusted to Defendants with the understanding that Defendants would safeguard this information against disclosure; (d) loss of the benefit of the bargain with Defendants to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect Plaintiff's Private Information; and (e) continued risk to Plaintiff's Private Information, which remains in the possession of Defendants and which is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendants.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

C. Cybercriminals Have Used and Will Continue to Use Plaintiff's Private Information to Defraud Them

31. Private Information is of great value to hackers and cybercriminals, and the data stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiff and the Class Members and to profit off their misfortune.

32. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[12] For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[13] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

33. Social Security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[14]
>
> [Emphasis added.]

---

[12] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[13] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[14] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

34. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[15]

35. This was a financially motivated Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack against companies like Kaye-Smith is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[16] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[17]

36. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, they ***will*** use it.[18]

37. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen 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.[19]

---

[15] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.
[16] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.
[17] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[18] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.
[19] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

38. For instance, with a stolen Social Security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[20]

39. The ramifications of Defendants' failure to keep its Class Members' Private Information secure are long lasting and severe. Once that information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

40. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available.

41. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened. [21] This gives thieves ample time to, for example, seek multiple medical treatments under the victim's name. Forty percent of consumers found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that were incurred in their names.[22]

42. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[23]

---

[20] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[21] *See* Medical ID Theft Checklist, *available at:* https://www.identityforce.com/blog/medical-id-theft-checklist-2.

[22] Experian, *The Potential Damages and Consequences of Medical Identify Theft and Healthcare Data Breaches ("Potential Damages")*, *available at:* https://www.experian.com/assets/data-breach/white-papers/consequences-medical-id-theft-healthcare.pdf.

[23] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

43. As a direct and proximate result of the Data Breach, Plaintiff and the Class have had their Private Information exposed, have suffered harm as a result, and have been placed at an imminent, immediate, and continuing increased risk of further harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, following Federal Trade Commission checklists, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps.

44. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent credit inquiries and cards being opened in their names;

b. Trespass, damage to, and theft of their personal property including Private Information;

c. Improper disclosure of their Private Information;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and having been already misused;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Private Information and that identity thieves have already used that information to defraud other victims of the Data Breach;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

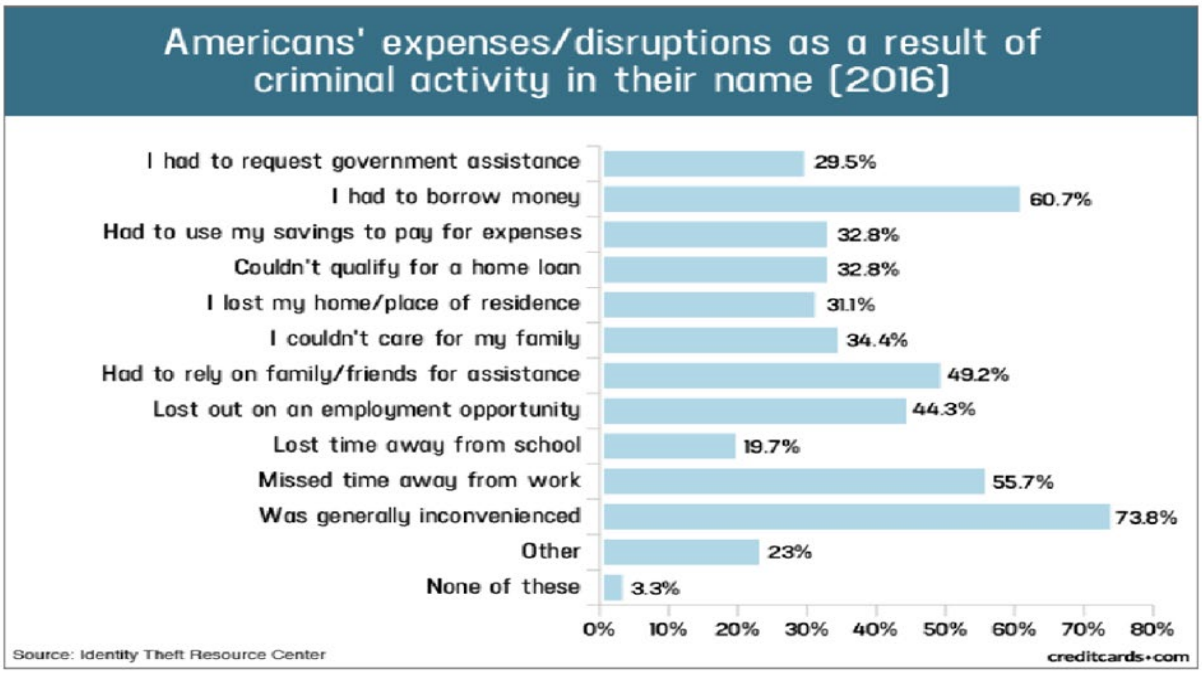
h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class members' personal information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Private Information; and

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

45. Below is a chart that shows the kinds of expenses and disruptions that victims of identity theft experience[24]:



[24] Jason Steele, *Credit Card and ID Theft Statistics*, CREDITCARDS.COM (Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

46. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown itself wholly incapable of protecting Plaintiff's Private Information.

47. Plaintiff and Class Members also have an interest in ensuring that their personal information that was provided to Kaye-Smith is removed from Kaye-Smith's unencrypted files.

48. Defendant itself acknowledged the harm caused by the Data Breach because it offered Plaintiff and Class Members an inadequate 12 or 24 months of identity theft repair and monitoring services. This limited identity theft monitoring is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk.[25]

49. Defendant further acknowledged, in its breach notification letter, that, in response to the Data Breach, Kaye-Smith "has enhanced its security measures and monitoring."[26] BECU similarly advised that it "worked with the vendor and a forensics firm before resuming services to improve the security of the vendor's environment as well as its effectiveness at preventing and detecting future cybersecurity incidents."[27]

50. The letters further acknowledged that the Data Breach would cause inconvenience to affected individuals by providing numerous actions for Class Members to take in an attempt to mitigate the harm caused by the Data Breach and that financial harm would likely occur. For example, the BECU letter states: "We recommend that you regularly review your account activity and periodically obtain your credit report from one or more of the national credit reporting companies… When you receive your credit reports, review them carefully. Look for accounts or

---

[25] *See* https://www.mass.gov/doc/assigned-data-beach-number-28266-kaye-smith-enterprises-inc/download.
[26] *Id.*
[27] *See* Exhibit 1, attached hereto.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

creditor inquiries…. We recommend that you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities....” [28]

51. At Kaye-Smith’s and BECU’s suggestion, Plaintiff is desperately trying to mitigate the damage that Kaye-Smith has caused him. Given the kind of Private Information Kaye-Smith made accessible to hackers, however, Plaintiff is certain to incur additional damages. Because identity thieves have his Private Information, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[29]

52. None of this should have happened.

D. Defendants were Aware of the Risk of Cyber Attacks

53. Data security breaches have dominated the headlines for the last two decades. And it doesn’t take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[30] Yahoo,[31] Marriott International,[32] Chipotle, Chili’s, Arby’s,[33] and others.[34]

---

[28] *Id.*

[29] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

[30] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[31] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[32] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[33] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[34] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

54. Companies providing services to the healthcare industry, such as Kaye-Smith, have been prime targets for cyberattacks. As early as August 2014, the FBI specifically warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[35]

55. Kaye-Smith should certainly have been aware, and indeed was aware, that it was at risk for a data breach that could expose the Private Information that it collected and maintained.

56. Thus, Kaye-Smith recognized it had a duty to use reasonable measures to protect the Private Information that it collected and maintained. Yet, it appears that Kaye-Smith did not meaningfully or comprehensively use the reasonable measures, including the measures it claims to utilize.

57. Kaye-Smith was clearly aware of the risks it was taking and the harm that could result from inadequate data security.

58. BECU should have certainly been aware Kaye-Smith was at risk for a data reach that could expose the Private information provided to Kaye-Smith.

59. BECU was clearly aware of the risks and the harm that could result from inadequate date security Kaye-Smith, in which it provided Plaintiff's and Class Members Private Information to.

E. Defendants Could Have Prevented the Data Breach

[35] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

60. Data breaches are preventable.[36] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[37] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[38]

61. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[39]

62. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[40] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming

---

[36] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[37] *Id.* at 17.
[38] *Id.* at 28.
[39] *Id.*
[40] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

63. Upon information and belief, Kaye-Smith failed to maintain many reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Kaye-Smith also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity readiness.

64. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[41]

65. To prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

---

[41] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[42]

[42] *Id.* at 3-4.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

66. Further, to prevent and detect malware attacks, including the malware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[43]

67. In addition, to prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise;
- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
- **Build credential hygiene**
  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events
- **Harden infrastructure**
  - Use Windows Defender Firewall

[43] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://us-cert.cisa.gov/ncas/tips/ST19-001.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[44]

68. Given that Defendants was storing the Private Information of many individuals, Defendants could and should have implemented all of the above measures to prevent and detect ransomware attacks.

69. Specifically, among other failures, Kaye-Smith had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[45] Indeed, the United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information, stating "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[46]

70. In sum, this Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all confidential information. Further, the Data Breach could have likely been prevented had Defendants utilized appropriate malware prevention and detection technologies.

71. BECU was negligent in its failure to not ensure Kaye-Smith had the proper security measures to store Plaintiff's and Class Members' confidential Private Information.

---

[44] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

[45] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, Aug. 14, 2018, https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

[46] "Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

F. Defendants Responses to the Data Breach are Inadequate to Protect Plaintiff and the Class

72. Defendants failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

73. Defendants stated that the Data Breach was discovered in or around May 2022. And yet, Plaintiff did not receive notification until July 25, 2022—months after Defendants learned of the Data Breach. Even then, Defendants failed to inform Plaintiff and Class Members exactly what information was exposed in the Data Breach, leaving Plaintiff and Class Members unsure as to the scope of information that was compromised.

74. During these intervals, the cybercriminals were exploiting the information while Kaye-Smith was secretly still investigating the Data Breach.

75. If Kaye-Smith had investigated the Data Breach more diligently and reported it sooner, Plaintiff and the Class could have taken steps to protect themselves sooner and to mitigate the damages caused by the Breach.

IV. CLASS ACTION ALLEGATIONS

76. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

77. Plaintiff brings this action against Kaye-Smith and BECU on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class and the state subclass (collectively, the "Class") defined as follows:

> Nationwide Class
> All persons whose Private Information was compromised as a result of the Data Breach.
>
> Washington Subclass
> All persons residing in Washington whose Private Information was compromised as a result of the Data Breach.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

78. Excluded from the Class are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

79. Plaintiff reserves the right to amend the above definitions or to propose additional subclasses in subsequent pleadings and motions for class certification.

80. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

81. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable.

82. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Kaye-Smith's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of Kaye-Smith.

83. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

84. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress Kaye-Smith's wrongdoing. Even if Class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

85. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendants engaged in the wrongful conduct alleged herein;

b. Whether Defendants failed to adequately safeguard Plaintiff's and the Class's Private Information;

c. Whether Defendants owed a duty to Plaintiff and the Class to adequately protect their Private Information, and whether it breached this duty;

d. Whether Defendants breached their duties to Plaintiff and the Class as a result of the Data Breach;

e. Whether Defendants failed to provide adequate cyber security;

f. Whether Defendants knew or should have known that its computer and network security systems were vulnerable to cyber attacks;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

g. Whether Defendants conduct, including their failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Kaye-Smith was negligent in permitting unencrypted Private Information of vast numbers of individuals to be stored within its network;

i. Whether BECU was negligent in permitting unencrypted Private Information of vast numbers of individuals to be stored within Kaye-Smith's network;

j. Whether Defendants were negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach to include former employees, applicants, and business associates;

k. Whether Defendants failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

l. Whether Kaye-Smith continues to breach duties to Plaintiff and the Class;

m. Whether Plaintiff and the Class suffered injury as a proximate result of Defendants' negligent actions or failures to act;

n. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

o. Whether Defendants' actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

V. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of all Plaintiffs and the Class)

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

86. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

87. Defendant Kaye-Smith solicited, gathered, and stored the Private Information of Plaintiff and the Class.

88. BECU solicited, gathered, and sent the Private information of Plaintiff and the Class to Kaye-Smith to be stored.

89. Defendants had full knowledge of the sensitivity of the Private Information it maintained and of the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed. Defendants had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and the Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their Private Information that was in BECU's or Kaye-Smith's possession. As such, a special relationship existed between BECU and the Plaintiff and the Class and bwtween Kaye-Smith and Plaintiff and the Class.

90. Defendants were well aware of the fact that cybercriminals routinely target corporations, particularly those servicing the health industry, through cyberattacks in an attempt to steal the collected Private Information.

91. Defendants owed Plaintiff and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

92. Defendants' duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

93. Defendants had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to cyberattacks, including by encrypting documents containing Private Information, by not permitting documents containing unencrypted Private Information to be maintained on its systems, and other similarly common-sense precautions when dealing with sensitive Private Information. Additional duties that Kaye-Smith and BECU owed Plaintiff and the Class include:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Private Information in its possession;
b. To protect the Private Information in its possession using reasonable and adequate security procedures and systems;
c. To adequately and properly audit and test its systems;
d. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;
e. To train its employees not to store Private Information for longer than absolutely necessary;
f. To implement processes to quickly detect a data breach, security incident, or intrusion; and
g. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

94. Plaintiff and the Class were the intended beneficiaries of Defendant's duties, creating special relationships between them and Kaye-Smith and between them and BECU. Defendant was in a position to ensure that its systems were sufficient to protect the Private Information that Plaintiff and the Class had entrusted to it.

95. Defendants breached their duties of care by failing to adequately protect Plaintiff's and Class Members' Private Information. Defendants breached their duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit and test its computer systems to avoid cyberattacks;

d. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information, including maintaining it in an encrypted format;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's Private Information;

f. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

g. Failing to abide by reasonable retention and destruction policies for Private Information it collects and stores; and

h. Failing to promptly and accurately notify Plaintiff and Class Members of the Data Breach that affected their Private Information.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

96. Defendants' willful failures to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

97. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

98. The damages Plaintiff and the Class have suffered (as alleged above) were and are reasonably foreseeable.

99. The damages Plaintiff and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

100. Plaintiff and the Class have suffered injury, including as described in Section IV.B, *supra*, and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of all Plaintiffs and the Class)

101. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

102. Through the use of Plaintiff's and Class Members' Private Information, Defendant received monetary benefits.

103. Defendants collected, maintained, and stored the Private Information of Plaintiff and Class Members and, as such, Defendants had direct knowledge of the monetary benefits conferred upon it by Plaintiff and Class Members.

104. Defendants appreciated that a monetary benefit was being conferred upon them by Plaintiff and Class Members and accepted that monetary benefit.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

105. However, acceptance of the benefit under the facts and circumstances described herein, make it inequitable for Defendants to retain that benefit without payment of the value thereof. Specifically, Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant Kaye-Smith instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

106. Under the principle of equity and good conscience, Defendants should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members because Kaye-Smith failed to implement the appropriate data management and security measures, and BECU failed to ensure the appropriate data management and security measures were in place.

107. Defendants acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

108. If Plaintiff and Class Members knew that Defendant had not secured their Private Information, they would not have agreed to allow Defendants to have or maintain their Private Information.

109. As a direct and proximate result of Kaye-Smith''s decision to profit rather than provide adequate data security, and as a ddirect and proximate cause of BECU's failure to ensure Kaye-Smith provided adequate data security, Plaintiff and Class members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Kaye-Smith reasonably should have expended on data security measures to secure Plaintiff's Private Information, (ii) time

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

and expenses mitigating harms, (iii) diminished value of the Private Information, (iv) harms as a result of identity theft; and (v) an increased risk of future identity theft.

110. Defendants, upon information and belief, have therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendants to retain the benefits it derived as a consequence of its wrongful conduct.

111. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

THIRD CAUSE OF ACTION
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On Behalf of the Nationwide Class)

112. Plaintiff incorporates by reference the foregoing paragraphs as if fully set forth herein.

113. Kaye-Smith entered into various contracts with its customers, including BECU, to perform services that include, but are not limited to, processing and servicing of third-party information.

114. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class members were the intended third-party beneficiaries of the contracts entered into between Defendants and their clients. Indeed, Defendants knew that if they were to breach these contracts with its customers, Plaintiff and Class members would be harmed.

115. Defendants breached the contracts it entered into with BECU and its other customers by, among other things, failing to (i) use reasonable data security measures, and (ii)

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

implement adequate protocols and employee training sufficient to protect the Private Information from unauthorized disclosure to third parties.

116. BECU required Plaintiff and Class Members entrust BECU with Private Information. BECU provided the Private Information to Kaye-Smith for storing, without ensuring adequate data security was in place.

117. As foreseen, Plaintiff and the Class were harmed by Defendants' breach of contracts with their clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

118. Plaintiff and Class members are also entitled to their costs and attorney's fees incurred in this action.

FOURTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of all Plaintiffs and the Class)

119. Plaintiff incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

120. Defendants required Plaintiff and Class Members to provide, or authorize the transfer of, their Private Information in order for Defendants to provide services. In exchange, Defendants entered into implied contracts with Plaintiff and Class Members in which Defendants agreed to comply with its statutory and common law duties to protect Plaintiff's and Class members' Private Information and to timely notify them in the event of a data breach.

121. Plaintiff and Class Members would not have provided their Private Information to Defendants had they known that Defendants would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

122. Plaintiff and Class Members fully performed their obligations under their implied contracts with Defendants.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

123. Defendants breached the implied contracts by failing to safeguard Plaintiff's and Class members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

124. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendant's breach of its implied contracts with Plaintiff and Class members.

FIFTH CAUSE OF ACTION
VIOLATION OF WASHINGTON CONSUMER PROTECTION ACT
RCW 19.86.010, *et seq.*,
(On Behalf of Plaintiff and the Washington Subclass)

125. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

126. Defendant Kaye-Smith and Defendant BECU are each a "person" within the meaning of the Washington Consumer Protection Act, RCW 19.86.010 and it conducts "trade" and "commerce" within the meaning of RCW 19.86.010(2).

127. Plaintiff and the Class are "persons" within the meaning of RCW 19.86.010(1).

128. Defendants engaged in unfair or deceptive acts or practices in the conduct of its business by through the conduct set forth throughout this Complaint. These unfair or deceptive acts or practices include, without limitation, the following:

a. Failing to adequately secure Plaintiff's and Class members' Private Information from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of Plaintiff's and Class members' Private Information in a manner highly offensive to a reasonable person;

c. Enabling the disclosure of Plaintiff's and Class members' Private Information without their informed, voluntary, affirmative, and clear consent;

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

d. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' Private Information; and

e. Failing to disclose the Data Breach in a timely and accurate manner.

129. Defendants' systematic acts or practices are unfair because these acts or practices (1) caused substantial financial injury to Plaintiffs' and Class members; (2) are not outweighed by any countervailing benefits to consumers or competitors; and (3) are not reasonably avoidable by consumers.

130. Defendant's systematic acts or practices are unfair because the acts or practices are immoral, unethical, oppressive, and/or unscrupulous.

131. Defendant's systematic acts or practices are deceptive because they were, and are capable of, deceiving a substantial portion of the public.

132. Defendant's unfair and deceptive acts or practices have repeatedly occurred in trade or commerce within the meaning of RCW 19.86.010 and RCW 19.86.020.

133. The acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

134. Defendant's unfair or deceptive acts or practices impact the public interest because they have injured Plaintiff and Class members.

135. As a direct and proximate result of Defendant's unfair or deceptive acts or practices, Plaintiff and Class members have suffered injury in fact and lost money.

136. As a result of Defendants' conduct, Plaintiff and Class members have suffered actual damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased and imminent risk of fraud and identity theft, the lost value of their Private Information, and other economic and non-economic harm.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

137. Plaintiff and the Class are therefore entitled to legal relief against Defendants, including recovery of nominal damages, actual damages, treble damages, injunctive relief, attorneys' fees and costs, and such further relief as the Court may deem proper.

138. Plaintiff and the Class are also entitled to injunctive relief in the form of an order prohibiting Defendants from engaging in the alleged misconduct and such other equitable relief as the Court deems appropriate.

139. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

140. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

141. As previously alleged and pleaded, Defendant owes duties of care to Plaintiff and Class Members that requires it to adequately secure their Private Information.

142. Defendants still possesses the Private Information of Plaintiff and the Class Members.

143. Defendants have not satisfied their obligations and legal duties to Plaintiff and the Class Members.

144. Kaye-Smith has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendants from reversing these changes once it has weathered the increased public attention resulting from this Breach, and to once again place profits above protection.

145. Plaintiff, therefore, seeks a declaration (1) that Kaye-Smith's existing security measures do not comply with its obligations and duties of care to provide adequate security, and

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

(2) that to comply with its obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendants to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering Defendants to significantly increase its spending on cybersecurity including systems and personnel;

c. Ordering Defendants to engage third-party security auditors and internal personnel to run automated security monitoring;

d. Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

e. Ordering that Defendants segments Plaintiff's and the Class's Private Information by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

f. Ordering that Defendants cease storing unencrypted Private Information on its systems;

g. Ordering that Defendants conduct regular database scanning and securing checks;

h. Ordering Defendants to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

i. Ordering Defendants to implement and enforce adequate retention policies for Private Information, including destroying, in a reasonably secure manner, Private Information once it is no longer necessary for it to be retained; and

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

j. Ordering Defendants to meaningfully educate its current, former, and prospective employees about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendants to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Complaint.

EMERY | REDDY, PLLC
600 Stewart Street, Suite 1100
Seattle, WA 98101
PHONE: (206) 442-9106 • FAX: (206) 441-9711

DATED: February 17, 2023.

EMERY | REDDY, PLLC

/s/ Timothy W. Emery
/s/ Patrick B. Reddy

TIMOTHY W. EMERY
WSBA No. 34078
PATRICK B. REDDY
WSBA No. 34092
EMERY REDDY, PLLC
600 Stewart St., Ste 1100
Seattle, WA 98101
Telephone: (206) 442-9106
Fax: (206) 441-9711
Email: emeryt@emeryreddy.com
Email: reddyp@emeryreddy.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
Email: wbf@federmanlaw.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108
Telephone: (405) 389-4989
Email: abm@murphylegalfirm.com

**pro hac vice request* forthcoming

Counsel for Plaintiff and the Putative Class

EXHIBIT 1

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

40058913000145143O
000 0004243 00000000 0001 0002 02122 INS: 0 0
RICHARD C. KREETING
[redacted]

July 25, 2022

Important Privacy Protection Notification. Please read this entire letter.

Dear Richard C. Krefting:

At BECU, we value your business and respect the privacy of your information, which is why we are writing to let you know about a vendor network security incident that involves your personal information. We encourage you to read this entire letter because it contains important information concerning the security of your account(s) at BECU. It also includes our offer to provide you with one year of credit monitoring protection at no cost to you unless otherwise required by local law. We take the protection of your information very seriously and are contacting you directly to explain the circumstances of the incident. To learn more, visit **becu.org/vendor-incident**.

What happened?
On June 6, 2022, BECU was informed that its printing vendor had experienced a network security incident. At that time, BECU took immediate measures to protect member information by suspending services with the vendor. After the incident occurred, the vendor indicated that some BECU member information in process at the time of the incident was potentially involved. On July 5, 2022, we were able to determine that your personal information was involved after an independent forensics firm had analyzed the compromised data. We sincerely apologize for any inconvenience or concern this incident may cause.

What information was involved?
The information involved may have included your name, address, account number(s), credit score, and Social Security number.

What we are doing.
The security of accounts and the protection of personal information – for you and all our members – are top priorities at BECU. We are committed to ensuring the security of your personal information. BECU worked with the vendor and a forensics firm before resuming services to improve the security of the vendor's environment as well as its effectiveness at preventing and detecting future cybersecurity incidents.

We understand you may have concerns, so we have secured Equifax Credit Watch™ Gold to provide you credit monitoring protection at no cost for one (1) year unless otherwise required by local law.

To take advantage of this offer, go to **www.equifax.com/activate**. Enter your unique Activation Code: [redacted] then click **Submit** and follow these steps:

1. **Register:** Complete the form with your contact information and click **Continue**.
   Note: If you already have a myEquifax account, click **Sign in here** under the Let's get started header. Once you have successfully signed in, skip to the Checkout page in Step 4.
2. **Create Account:** Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout page. Click **Sign Me Up** to finish enrolling. The confirmation page shows your completed enrollment. Click **View My Product** to access the product features.
5. **Enrollment Deadline:** October 31, 2022

Special note for minors affected by this incident: The same services referred to above may not be available to affected minors. As an alternative, you can contact our member support line at 877-390-2571 to request an Equifax Minor Monitoring product.

What you can do.
We sincerely apologize for any inconvenience or concern this incident may cause. We recommend that you regularly review your account activity and periodically obtain your credit report from one or more of the national credit reporting companies.

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are also two types of fraud alerts that 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 90 days.

You may have an extended alert placed on your credit report if you have already been a victim of identity theft with 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 calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 888-766-0008, www.equifax.com
Experian: 888-397-3742, www.experian.com
TransUnion: 800-680-7289, fraud.transunion.com

Credit Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent.

If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Because the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies, as specified below, to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

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, including the use of fraud alerts and security freezes. 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).

Residents of Massachusetts, Maryland, North Carolina, New York, Connecticut, and the District of Columbia can obtain more information about preventing and avoiding identity theft from their Attorneys General using the contact information below.

For Massachusetts residents: You are advised to report any suspected identity theft to law enforcement and that you have the right to obtain a police report.