THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA

IN RE: OVERBY-SEAWELL COMPANY CUSTOMER DATA SECURITY BREACH LITIGATION	Case No. 1:23-md-03056 SDG **CONSOLIDATED CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiffs Mariann Archer, Mark Samsel, Tim Marlowe, Melissa Urciuoli, James Urciuoli, Patrick Reddy, Jacint "Jay" Pittman, Joseph John Turowski, Jr., Teresa Turowski, Melissa D. Kauffman, Lebertus Vanderwerff, Adrianne Khanolkar, Dhamendra "DK" Khanolkar, and Joynequa West ("Plaintiffs") bring this Consolidated Class Action Complaint against Overby-Seawell Company ("OSC") and KeyBank National Association ("KeyBank" and collectively with OSC, "Defendants"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to

properly secure and safeguard personally identifiable information ("PII")[1] for resident mortgage clients of KeyBank and other lenders that utilized the services of OSC, including, but not limited to, their names, mortgage property addresses, mortgage account numbers and mortgage account information, phone numbers, property information, the first eight digits of Social Security numbers, and home insurance policy numbers and home insurance information.

2. According to KeyBank's website, it has approximately 1,000 full-service branches in 15 states and is "one of the nation's largest bank-based financial services companies, with assets of approximately $186 billion."[2]

3. According to OSC's website, it "is a leading provider of compliance-driven tracking technology and insurance products and services for lenders, mortgage servicers and property investors."[3]

4. Both Defendants are sophisticated financial entities and regularly maintain consumer information they know to be sensitive. Moreover, they are aware of the consequences that would result to those consumers if the information were to be compromised and their corresponding obligation to protect against such

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.
[2] *See* https://www.key.com/about/company-information/key-company-overview.html (last visited June 8, 2023).
[3] *See* https://www.oscis.com/who-we-are/ (last visited June 8, 2023).

compromise.

5. In its Privacy Notice for Consumers in effect at the time of the Data Breach (the "KeyBank Privacy Notice"), revised February 4, 2020, KeyBank represents that "At Key, we are committed to safeguarding personal information. We use physical, technical, and administrative security measures that comply with applicable federal and state laws and regulations."[4]

6. In its Privacy Policy (the "OSC Privacy Policy"), OSC represents that "we have in place physical, electronic, and procedural safeguards in order to protect any nonpublic personal information we maintain regarding our Participants."[5]

7. Prior to and through July 5, 2022, KeyBank, and in furtherance of its operations as a financial institution, obtained the PII of Plaintiffs and Class Members, its customers, and shared that PII, unencrypted, with OSC, which stored that PII, unencrypted, in an Internet-accessible environment on OSC's network.

8. On or before August 4, 2022, OSC learned that an unauthorized external party gained remote access to its network and, on July 5, 2022, acquired information from a number of OSC clients, including the PII of Plaintiffs and Class Members that OSC obtained from KeyBank (the "Data Breach").

---

[4] *See* https://web.archive.org/web/20221129172933/https://www.key.com/about/misc/online-privacy-statement.html (as published on November 29, 2022)

[5] *See* https://www.oscis.com/privacy/ (last visited June 8, 2022).

9. Upon information and belief, Defendants were targeted in the cyberattack due to the high volume of sensitive PII that they collected and maintained on their computer networks and/or systems and the high value of that information to cyber criminals in facilitating identity theft and fraud.

10. On or around August 26, 2022, KeyBank began notifying various states Attorneys General of the Data Breach.

11. On or around August 26, 2022, KeyBank began notifying Plaintiffs and Class Members of the Data Breach.

12. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendants assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. KeyBank admits that the unencrypted PII obtained by an unauthorized external party includednames, mortgage property addresses, mortgage account numbers and mortgage account information, phone numbers, property information, the first eight digits of Social Security numbers, and home insurance policy numbers and home insurance information.

13. The exposed PII of Plaintiffs and Class Members was targeted due to its value on the dark web. Hackers target and sell to criminals the unencrypted, unredacted PII that they exfiltrate from companies like Defendants. Plaintiffs and Class Members now face a present and continuing lifetime risk of: (i) identity theft,

which is heightened here by the loss of Social Security numbers in conjunction with other sensitive information; and (ii) the sharing and detrimental use of their sensitive information over which they have now been deprived of control.

14. The PII was targeted and compromised due to Defendants' negligent and/or careless acts and omissions and failure to protect the PII of Plaintiffs and Class Members. In addition to Defendants' failure to prevent the Data Breach, Defendants waited several weeks after the Data Breach occurred to report it to the states' Attorneys General and affected individuals. Defendants have also purposefully maintained as secret the specific vulnerabilities and root causes of the breach and have not informed Plaintiffs and Class Members of that information.

15. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

16. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failures to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendants' inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of

vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

17. Plaintiffs and Class Members have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the disclosure of their private information; (v) failure to receive the benefit of their bargains with Defendants related to their financial products; (vi) nominal damages; (vii) the continued and certainly increased risk to their PII, and damages in an amount equal to the cost of securing identity theft products to assisting in monitoring and protecting them from identity theft, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

18. Defendants disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized

disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

Plaintiff Mariann Archer

19. Plaintiff Mariann Archer is an adult individual and a natural person of New York residing in Oneida where she intends to stay. Plaintiff is a citizen of the State of New York.

20. Plaintiff Archer received a notice letter from Defendant KeyBank dated August 26, 2022, informing her of the Data Breach and the exposure of her PII.

21. The notice letter informed Plaintiff that her full name, mortgage property address, mortgage account number and mortgage account information, telephone number, property information, the first eight digits of her Social Security number, and her home insurance policy number and home insurance information were acquired by unauthorized third parties.

Plaintiff Mark Samsel

22. Plaintiff Mark Samsel is an adult individual and a natural person of

Ohio, residing in Lorain County, where he intends to stay. Plaintiff Samsel is a citizen of the State of Ohio.

23. Plaintiff Mark Samsel received a notice letter from Defendant KeyBank dated August 26, 2022, informing him of the Data Breach and the exposure of his PII.

24. The notice letter informed Plaintiff that his name, mortgage address, mortgage account number, phone number, first eight digits of his SSN, home insurance policy number, and home insurance information were acquired by unauthorized parties in the Data Breach.

Plaintiff Tim Marlowe

25. Plaintiff Tim Marlowe is an adult individual and a natural person of Ohio, residing in Clermont County, where he intends to stay. Plaintiff Marlowe is a citizen of the State of Ohio.

26. Plaintiff Marlowe received a notice letter from Defendant KeyBank dated August 26, 2022, informing him of the Data Breach and the exposure of his PII.

27. The notice letter informed Plaintiff that his name, first eight digits of Social Security Number, mortgage property address, mortgage account number, mortgage account information, phone number, property information, home insurance policy number, and home insurance information were acquired by

unauthorized third parties in the Data Breach.

Plaintiff Melissa Urciuoli

28. Plaintiff Melissa Urciuoli ("M. Urciuoli") is an adult individual and a natural person of Oregon, residing in Lane County, where she intends to stay. Plaintiff is a citizen of the State of Oregon.

29. Plaintiff M. Urciuoli received a notice letter from Defendant KeyBank dated August 26, 2022, informing her of the Data Breach and the exposure of her PII.

30. The notice letter informed Plaintiff M. Urciuoli that her name, mortgage property address, mortgage account number and mortgage account information, phone number, property information, the first eight digits of her Social Security number, and home insurance policy number and home insurance information were acquired by unauthorized third parties in the Data Breach.

Plaintiff James Urciuoli

31. Plaintiff James Urciuoli ("J. Urciuoli") is an adult individual and a natural person of Oregon, residing in Lane County, where he intends to stay. Plaintiff is a citizen of the State of Oregon.

32. Plaintiff J. Urciuoli received a notice letter from Defendant KeyBank dated August 26, 2022, informing him of the Data Breach and the exposure of his PII.

33. The notice letter informed Plaintiff J. Urciuoli that his name, mortgage property address, mortgage account number and mortgage account information, phone number, property information, the first eight digits of his Social Security number, and home insurance policy number and home insurance information were acquired by unauthorized third parties in the Data Breach.

Plaintiff Patrick Reddy

34. Plaintiff Patrick Reddy is an adult individual and a natural person of Washington, residing in King County, where he intends to stay. Plaintiff is a citizen of the State of Washington.

35. Plaintiff Patrick Reddy received a notice letter from Defendant KeyBank dated August 26, 2022, informing him of the Data Breach and the exposure of his PII.

36. The notice letter informed Plaintiff Reddy that his full name, mortgage property address, mortgage account number and mortgage account information, telephone number, property information, the first eight digits of his Social Security number, and his home insurance policy number and home insurance information were acquired by unauthorized parties in the Data Breach.

Plaintiff Jacint Pittman

37. Plaintiff Jacint "Jay" Pittman is an adult individual and a natural person of Pennsylvania, residing in Allegheny County, where he intends to stay. Plaintiff

Pittman is a citizen of the State of Pennsylvania.

38. Plaintiff Pittman received a notice letter from Defendant KeyBank at some point between June and August 2022 informing him of the Data Breach and the exposure of his PII.

39. The notice letter informed Plaintiff Pittman that his name, property address, account number, account information, phone number, Social Security Number, and loan information were acquired by unauthorized parties in the Data Breach.

Plaintiffs Joseph John Turowski, Jr. and Teresa Turowski

40. Plaintiff Joseph John Turowski, Jr. and Plaintiff Teresa Turowski are adult individuals and natural persons of Pennsylvania, residing in Philadelphia, where they intend to stay. Turowski Plaintiffs are citizens of the State of Pennsylvania.

41. Joseph and Teresa received a notice letter from Defendant KeyBank dated August 26, 2022, informing them of the Data Breach and the exposure of their PII.

42. The notice letter informed Joseph and Theresa that the following personal information of theirs was acquired by unauthorized parties in the Data Breach: names, mortgage property, address, mortgage account number(s) and mortgage account information, phone numbers, property information, the first eight

digits of their Social Security numbers, home insurance policy number and home insurance information.

Plaintiff Melissa Kauffman

43. Plaintiff Melissa Kauffman is an adult individual and a natural person of Indiana, residing in Elkhart County, where she intends to stay. Plaintiff Kauffman is a citizen of the State of Indiana.

44. Plaintiff Melissa Kauffman received a notice letter from Defendant KeyBank informing her of the Data Breach and the exposure of her PII.

45. The notice letter informed Plaintiff that her personal information, including login credentials, were acquired by unauthorized parties in the Data Breach.

Plaintiff Lebertus Vanderwerff

46. Plaintiff Lebertus Vanderwerff is an adult individual and a natural person of New York, residing in Cayuga, where he intends to stay. Plaintiff Vanderwerff is a citizen of the State of New York.

47. Plaintiff Vanderwerff received a notice letter from KeyBank informing him of the Data Breach and the exposure of his PII.

48. The notice letter informed Plaintiff that his personal and account information were acquired by unauthorized parties in the Data Breach.

Plaintiff Adrianne Khanolkar

49. Plaintiff Adrianne Khanolkar is an adult individual and a natural person of California residing in Alameda County where she intends to stay. Plaintiff Khanolkar is a citizen of the State of California.

50. Plaintiff Adrianne Khanolkar received a notice letter from Defendant KeyBank dated August 26, 2022, informing her of the Data Breach and the exposure of her PII.

51. The notice letter informed Plaintiff that her name, mortgage property address, mortgage account number and mortgage account information, phone number, property information, the first eight digits of her Social Security number, and home insurance policy number and home insurance information were acquired by unauthorized parties in the Data Breach.

Plaintiff Dharmendra Khanolkar

52. Plaintiff Dharmendra "DK" Khanolkar is an adult individual and a natural person of California, residing in Alameda County, where he intends to stay. Plaintiff Khanolkar is a citizen of the State of California.

53. Plaintiff Dharmendra Khanolkar received a notice letter from Defendant KeyBank dated August 26, 2022, informing him of the Data Breach and the exposure of his PII.

54. The notice letter informed Plaintiff that his name, mortgage property address, mortgage account number and mortgage account information, phone

number, property information, the first eight digits of his Social Security number, and home insurance policy number and home insurance information were acquired by unauthorized parties in the Data Breach.

Plaintiff Joynequa West

55. Plaintiff Joynequa West is an adult individual and a natural person of the commonwealth of Pennsylvania, residing in Philadelphia, Pennsylvania, where she intends to stay. Plaintiff West is a citizen of the State of Pennsylvania.

56. Plaintiff West is a customer of Fulton Bank and provided her personal PII to Fulton Bank as a condition of receiving services from Fulton Bank. Fulton Bank in turn entrusted Plaintiff West's PII to OSC.

57. Plaintiff West received a letter from OSC on or about August 30, 2022, informing her of the Data Breach and the unauthorized access to her PII, including her name, telephone number, loan number, mailing and collateral address, loan amount and loan maturity date, and apparently her full Social Security number.

Defendant KeyBank National Association

58. Defendant KeyBank National Association is a National Association bank organized under the laws of the United States with a principal place of business in Cleveland, Ohio. KeyBank is a citizen of the State of Ohio.

59. Among other things, KeyBank originates and periodically sells commercial and residential mortgage loans but continues to service those loans for

the buyers of those mortgages.KeyBank and its bank holding company KeyCorp are one of the nation's largest banks and financial services companies, with KeyCorp having consolidated total assets of approximately $186.3 billion as of December 31, 2021.

60. As of December 31, 2021, KeyBank had approximately 999 full-service retail banking branches and a network of 1,317 ATMs in 15 states.

61. KeyBank provides traditional banking and lending services to its customers including originating and/or servicing residential mortgages. According to KeyCorp's SEC Form 10-K for fiscal year ending December 31, 2021, filed on February 22, 2022 ("2021 10-K"):

> Through KeyBank and certain other subsidiaries, we provide a wide range of retail and commercial banking, commercial leasing, investment management, consumer finance, student loan refinancing, commercial mortgage servicing and special servicing, and investment banking products and services to individual, corporate, and institutional clients through two major business segments: Consumer Bank and Commercial Bank.

62. According to KeyCorp's 2021 10-K, its "residential mortgage portfolio is comprised of loans originated by our Consumer Bank primarily within our 15-state footprint and is the largest segment of our consumer loan portfolio as of December 31, 2021, representing approximately 51% of consumer loans."

Defendant Overby-Seawell Company

63. The Overby-Seawell Company is a Georgia corporation with its

principal place of business in Kennesaw, Georgia.

64. OSC is a technology services vendor of KeyBank that provides KeyBank with ongoing verification for its residential mortgage clients' maintenance of property insurance, which are required for homeowners to maintain based on the terms of their KeyBank mortgages.

65. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of other such responsible parties when their identities become known.

66. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

67. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiffs, is a citizen of a state different from OSC to establish minimal diversity.

68. OSC is a citizen of Georgia because it is a Georgia corporation and its principal place of business is in Kennesaw, Georgia. Thus, the Northern District of Georgia has general jurisdiction over OSC.

69. The Northern District of Georgia has personal jurisdiction over OSC because it conducts substantial business in Georgia and this District.

70. The Northern District of Georgia has personal jurisdiction over KeyBank because it shared Plaintiffs' and Class Members' PII with OSC in Georgia and this District.

71. Venue is proper in this District under 28 U.S.C. §1391(b) because OSC operates in this District, KeyBank provided and entrusted Plaintiffs' and Class Members' PII to OSC in this District, and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

72. Plaintiffs and Class Members, who are past and current clients of KeyBank and others, provided and entrusted KeyBank and the others with sensitive and confidential information, including but not limited to their names, mortgage property addresses, mortgage account numbers and mortgage account information, phone numbers, property information, Social Security numbers, and home insurance policy numbers and home insurance information.

73. OSC is a provider of efficiency and compliance solutions offering services in the areas of regulatory and governance best practices, real time data tracking, operations outsourcing, and insurance and risk management. OSC contracts with companies like KeyBank and uses the PII of their consumers to provide its services. On information and belief, OSC' contracts with the entities that provided the PII of Plaintiffs and Class Members contained specific obligations to safeguard the PII it collected and maintained as part of its business practices.

74. As a condition of being a past or current client of KeyBank, KeyBank required that Plaintiffs and Class Members entrust KeyBank with highly confidential PII. Other companies similarly served by OSC also collected the PII of consumers, some of whom are Class Members and entrusted to OSC that PII.

75. KeyBank and others shared the PII of Plaintiffs and Class Members with OSC, which stored the PII unencrypted and on its Internet-accessible network.

76. Plaintiffs and Class Members relied on the companies that entrusted their PII to OSC, and on OSC itself, to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the integrity and confidentiality of their PII and demand security to safeguard their PII.

77. In addition to Plaintiffs and Class Members' complete dependence on KeyBank and OSC to protect their PII, because this was a readily foreseeable and

preventable data breach and Defendants represented that they valued and would protect the PII of Plaintiffs and Class Members, Defendants had duties to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Data Breach

78. On or about August 26, 2022, KeyBank sent Plaintiffs and Class Members a *Notice of Vendor Security Incident*[6] in which KeyBank informed Plaintiffs and other Class Members that:

> **What happened?**
>
> On August 4, 2022, we were contacted by Overby-Seawell Company (OSC), regarding a cybersecurity incident affecting KeyBank clients. OSC is a vendor that provides KeyBank ongoing verification that our residential mortgage clients are maintaining property insurance. OSC informed us that an unauthorized external party had gained remote access to their network and on July 5, 2022 acquired certain information from a number of OSC clients, including certain personal information of KeyBank clients.
>
> **What information was involved?**
>
> Information pertaining to your KeyBank mortgage was part of the data acquired from OSC systems. The specific information acquired includes your:
> - name
> - mortgage property address

[6] Exhibit 1 (sample notice filed with Montana attorney general's office), *available at* https://media.dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-517.pdf (last visited Sept. 6, 2022).

- mortgage account number(s) and mortgage account information
- phone number
- property information
- the first eight digits of your Social Security number
- home insurance policy number and home insurance information

***

What are we doing?

OSC is investigating this incident with the assistance of third-party cybersecurity experts. They have deployed enhanced security monitoring tools across their network and notified the Federal Bureau of Investigation (FBI) of this incident.[7]

79. On or about August 26, 2022, KeyBank notified various state Attorneys General of the Data Breach, including the Attorneys General of Massachusetts and Montana, and provided them "sample" notices of the Data Breach. KeyBank notified the Attorney General of Massachusetts that 4,588 Massachusetts residents were affected by the Data Breach and notified the Attorney General of Montana that 228 Montana residents were affected by the Data Breach.

80. KeyBank admitted in the *Notice of Vendor Security Incident*, the letters to the Attorneys General, the "sample" notices of the Data Breach, and the Website Notice that an unauthorized actor obtained sensitive information about Plaintiffs and Class Members, including their names, mortgage property addresses, mortgage

[7] *Id.*

account number(s) and mortgage account information, phone numbers, property information, the first eight digits of Social Security numbers, and home insurance policy numbers and home insurance information.

81. In response to the Data Breach, KeyBank claims that OSC has "deployed enhanced security monitoring tools across their network."[8] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

82. As a result of the Data Breach, the unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web, or fall into the hands of companies that will use the detailed PII for targeted marketing without the consent of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

83. Because Defendants had duties to protect Plaintiffs' and Class Members' PII, Defendants should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

84. In the years immediately preceding the Data Breach, Defendants knew

[8] *Id*.

or should have known that OSC's computer systems were a target for cybersecurity attacks, including attacks involving data theft, because warnings were readily available and accessible via the internet. In addition to articles in the public press about the extensive number of data breaches affecting companies throughout all industries, including the financial industry, governmental agencies have constantly sent and published notices of the need for companies, including those in the financial industry to carefully safeguard the sensitive and valuable information collected from consumers.

85. On its website, KeyBank acknowledges that "[i]n recent years, government agencies and well-known corporations have experienced major data breaches" and that "[a]ny organization that collects personal information about employees, customers or other individuals can be a target."[9]

86. This readily available and accessible information confirms that, prior to the Data Breach, Defendants knew or should have known that (i) unauthorized actors were targeting companies such as OSC, (ii) unauthorized actors were aggressive in their pursuit of companies such as OSC, (iii) unauthorized actors were leaking corporate information on dark web portals, and (iv) unauthorized actors' tactics included threatening to release stolen data.

[9] *See* https://www.key.com/businesses-institutions/business-expertise/articles/protecting-your-companys-data-privileged-access.html (last visited Sept. 6, 2022).

87. Given KeyBank's knowledge that the sensitive information it maintained would be targeted by hackers, KeyBank had a duty to convey that information to OSC and to ensure that OSC instituted appropriate data security procedures to guard against this threat.

88. In light of the information readily available and accessible on the internet before the Data Breach, KeyBank, having elected to share the unencrypted PII of consumers with OSC, and OSC, having elected to store that PII and other similar PII from other entities in an Internet-accessible environment, had reason to be on guard for the targeting and exfiltration of the PII at issue here. Defendants had cause to be particularly on guard against such an attack as a result of their foreknowledge as demonstrated in their public representations.

89. Prior to the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

90. Prior to the Data Breach, Defendants knew or should have known that they should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Data Breaches are Preventable.

91. To prevent and detect cyber-attacks and/or ransomware attacks

Defendants could and should have implemented, as recommended by the United States Government, 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.
- 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.[10]

92. To prevent and detect cyber-attacks or ransomware attacks 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;

[10] https://www.meritalk.com/articles/fbi-high-impact-ransomware-attacks-threaten-u-s-businesses-and-organizations/

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
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[11]

93. Given that Defendants were storing the PII of so many individuals, Defendants could and should have implemented all the above measures to prevent and detect cyberattacks, and their failure to do so was negligent if not reckless

94. The occurrence of the Data Breach evidences that Defendants failed to adequately implement one or more of the above measures to prevent cyberattacks,

[11] *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/ (last visited June 8, 2023).

resulting in the Data Breach and the exposure of the PII of Plaintiffs and Class Members.

Defendants Failed to Comply with FTC Guidelines

95. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

96. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer 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 to correct any security problems.[12]

97. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large

[12] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited June 8, 2022).

amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[13]

98. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

99. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

100. These FTC enforcement actions include actions against companies like Defendants.

101. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable

[13] *Id.*

measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

102. Defendants failed to properly implement basic data security practices.

103. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

104. Upon information and belief, Defendants were at all times fully aware of their obligation to protect the PII of their customers and clients' customers, Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendants Failed to Follow Industry Standards

105. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

106. Several best practices have been identified that, at a minimum, should be implemented by companies in possession of PII like Defendants, including but

not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which customers can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

107. Other best cybersecurity practices that are standard for companies in possession of PII include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

108. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

109. These foregoing frameworks are existing and applicable industry standards for companies in possession of PII, and upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Defendant failed to comply with the Gramm-Leach-Bliley Act

110. Defendants provide investment advice and other financial services and consumer financial products, including insurance, and are therefore subject to the Gramm-Leach-Bliley Act.

111. Defendants collect nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendants were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1 et seq., and are subject to numerous rules and regulations promulgated on the GLBA Statutes. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau ("CFPB") became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

112. Accordingly, Defendants' conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

113. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous."16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendants violated the Privacy Rule and Regulation P.

114. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining

these customers' PII and storing and/or sharing that PII on its network.

115. Defendant failed to adequately inform its customers that it was storing and/or sharing, or would store and/or share, the customers' PII on its inadequately secured network and would do so after the customer relationship ended.

116. The Safeguards Rule, which implements Section 501(b) of the GLBA,15 U.S.C. § 6801(b), requires institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4. As alleged herein, Defendants violated the Safeguard

Rule.

117. Defendants failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of PII in its custody or control.

118. Defendants failed to design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

119. Defendants failed to adequately oversee service providers.

120. Defendants failed to evaluate and adjust its information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances.

The Data Breach was Foreseeable

121. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store PII, like Defendants, preceding the date of the breach.

122. Data breaches, including those perpetrated against financial entities that store PII in their systems, have become widespread.

123. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from

2020.[14]

124. The U.S. government, various U.S. and international law enforcement agencies, cybersecurity industry groups and laboratories, and numerous industry trade groups have issued warnings and guidance on managing and mitigating phishing and ransomware threats. There are industry best practices for cybersecurity related to phishing and ransomware, some of which are particularly effective.

125. For example, in 2019, both Microsoft and Google have publicly reported that using multi-factor authentication ("MFA") blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating "[t]ime to implement multi-factor authentication!"[15] An example of MFA implementation is receiving a text with a code when you input your username and password into a website; even if a cybercriminal knew your username and password, the cybercriminal would not be able to see the code on your phone and would thus be blocked from accessing your online account.

---

[14] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

[15] Matt Bromiley, *Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ [https://perma.cc/ZSW9-QUEW]. Matt Bromiley, *Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ [https://perma.cc/ZSW9-QUEW].

126. In this regard, implementing MFA "can block over 99.9 percent of account compromise attacks."[16]

127. Cyberattacks have become so notorious that the FBI and Secret Service issued an unprecedented warning in 2019 to potential targets so they were aware of, and prepared for, a potential attack.[17]

128. Cyberattacks and data breaches of financial services companies are especially problematic because of the potentially permanent disruption they cause to the daily lives of their customers. Stories of identity theft and fraud abound, with hundreds of millions of dollars lost by everyday consumers every year as a result of internet-based identity theft attacks.[18]

129. The U.S. Government Accountability Office ("GAO") released a report in 2007 regarding data breaches finding that victims of identity theft will face

---

[16] *What Is Multi-Factor Authentication (MFA)?*, Consensus Techs. (Sept. 16, 2020), https://www.concensus.com/what-is-multi-factor-authentication/#:~:text=The%20proof%20that%20MFA%20works,percent%20of%20account%20compromise%20attacks [https://perma.cc/RKT2-LX5Z].

[17] Kochman, *supra* n.171.

[18] Albert Khoury, *Scam alert: 5 most costly data breaches (plus 5 states most targeted)* (July 27, 2022), https://www.komando.com/security-privacy/most-costly-data-breaches/847800/

"substantial costs and time to repair the damage to their good name and credit record."[19]

130. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[20]

131. In light of recent high profile data breaches at industry leading companies, including, Microsoft (250 million records, December 2019), Capital One (98 million consumer's records, July 2019);Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendants knew or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

132. Additionally, as companies became more dependent on computer systems to run their business,[21] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and

---

[19] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf [https://perma.cc/GCA5-WYA5].

[20] *Id*.

[21] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

technical safeguards.[22]

133. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if OSC's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

134. Defendants could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiffs and Class Members. Alternatively, Defendants could have destroyed the data they no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

135. Defendants' negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

136. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

Plaintiffs and Class Members are under a Present and Continuing Risk of

[22] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

Identity Theft and Fraud

137. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[23] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[24]

138. 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 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.[25]

139. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information.

[23] 17 C.F.R. § 248.201 (2013).
[24] *Id*.
[25] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/Steps (last visited June 12, 2021) [https://perma.cc/ME45-5N3A].

Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

140. Plaintiffs' and Class Members' PII provided by consumers to a financial institution, typically provided under penalty of 18 U.S.C. § 1344, is accurate and of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

141. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

142. The fraudulent activity resulting from the Data Breach may not come to light for years.

143. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("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 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.[26]

144. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime. And because Social Security numbers, names, and, practically speaking, home addresses are immutable information, the PII stolen in this breach can be used to target Plaintiffs and Class Members for the remainder of their lives.

145. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[27]

---

[26] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last accessed Mar. 15, 2021).

[27] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18,

146. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

147. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. Moreover, because much of the information at issue here includes immutable data like Social Security numbers, names, and, for all practical purposes, home addresses, Plaintiffs' and Class Members' PII can be used to victimize them for the remainder of their lives.

148. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone

---

2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

numbers and emails) of Plaintiff and the other Class Members. And because the criminals here have either the full or the first eight numbers of Plaintiffs and Class Members' Social Security numbers, they can easily obtain the last four numbers, which are often used as identifiers, through techniques like social engineering.

149. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

150. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

151. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

152. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[28]

153. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

154. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[29]

---

[28] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 26, 2022).
[29] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-

155. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts, although cyber criminals can still use this information to develop synthetic identities and can engage if financial crimes. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

156. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[30]

157. Plaintiffs and Class Members now face a lifetime of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

158. The ramifications of Defendants' failure to keep secure the PII of

---

stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 26, 2022).

[30] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 26, 2022).

Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

159. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[31] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[32] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[33]

160. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[34]

---

[31] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 26, 2022).

[32] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2022).

[33] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Dec. 29, 2020).

[34] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

161. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[35,36]

162. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[37]

163. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[38]

164. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

165. Defendants were, or should have been, fully aware of the unique type and the significant volume of data contained in the PII that KeyBank shared with

---

[35] https://datacoup.com/

[36] https://digi.me/what-is-digime/

[37] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

[38] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sep. 13, 2022).

OSC, amounting to potentially thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

166. To date, OSC has offered Plaintiffs and Class Members only two years of personal information misuse detection and identity protection support through Equifax. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for the remainder of their lives in light of the PII at issue here.

167. That Defendants are encouraging Plaintiffs and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted individuals' PII was acquired, thereby subjecting Plaintiff and Class Members to a substantial and imminent threat of fraud and identity theft.

168. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Plaintiff Mariann Archer's Experience

169. Plaintiff Archer greatly values her privacy and Sensitive Information, especially when receiving loan and financial services. Plaintiff Archer has taken reasonable steps to maintain the confidentiality of her PII, and she has never

knowingly transmitted unencrypted PII over the internet or any other unsecured source.

170. Plaintiff Archer stores all documents containing PII in a secure location and destroys any documents she receives in the mail that contain any PII or that may contain any information that could otherwise be used to compromise her identity and financial accounts. Moreover, she diligently chooses unique usernames and passwords for her various online accounts. In addition, she does not release her birthdate or other PII on social media sites, etc., as a precautionary measure from identity fraud.

171. Plaintiff Archer only allowed Defendants to maintain, store, and use her PII because she believed that Defendants would use basic security measures to protect her PII, such as requiring passwords and multi-factor authentication to access databases storing her PII. As a result, Plaintiff's PII was within the possession and control of Defendants at the time of the Data Breach.

172. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

173. Plaintiff has been further injured by the damages to and diminution in value of her PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon

information and belief, later placed for sale on the dark web.

174. The Data Breach has also caused Plaintiff to suffer current and continuing injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

175. As a result of the actual harm she has suffered a present and continuing risk of harm, Plaintiff Archer has spent multiple hours dealing with the consequences of the Data Breach including checking her account and bank statements twice a week, reviewing her credit scores monthly, as well as her time spent verifying the legitimacy of the Notice of Data Breach, communicating with her bank, and researching multiple forms of security protection services. Since receiving the notice letter, Plaintiff Archer has also placed security freezes on her credit reports with Equifax, Experian, and TransUnion. Plaintiff Archer spent valuable time signing up for credit monitoring services through Equifax at Defendant's direction and reviews the reports she receives from the Equifax service monthly. This time has been lost forever and cannot be recaptured.

176. In addition to the present and continuing risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the notice letter, and self-monitoring her accounts and credit reports to ensure no

fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

177. Defendant KeyBank acknowledged the risk posed to Plaintiff and her PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years.

178. The present and continuing risk of harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

179. Plaintiff has a continuing interest in ensuring that Plaintiff's PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Mark Samsel's Experience

180. Plaintiff Mark Samsel is a cautious person and is therefore very careful about sharing his sensitive PII. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

181. Plaintiff Mark Samsel only allowed Defendants to maintain, store, and

use his PII because he believed that Defendants would use basic security measures to protect his PII, such as requiring passwords and multi-factor authentication to access databases storing his PII. As a result, Plaintiff's PII was within the possession and control of Defendants at the time of the Data Breach.

182. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

183. Plaintiff has been further injured by the damages to and diminution in value of his PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

184. The Data Breach has also caused Plaintiff to suffer present and continuing injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

185. In addition to the present and continued risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot

be recaptured, was spent at Defendants' direction.

186. Defendant KeyBank acknowledged the risk posed to Plaintiff and his/her/their PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years.

187. The present and continuing risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

188. Plaintiff has a continuing interest in ensuring that Plaintiff's PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Tim Marlowe's Experience

189. Plaintiff Marlowe is a cautious person and is therefore very careful about sharing his sensitive PII. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

190. Plaintiff Marlowe only allowed Defendants to maintain, store, and use his PII because he believed that Defendants would use basic security measures to

protect his PII, such as requiring passwords and multi-factor authentication to access databases storing his PII. As a result, Plaintiff's PII was within the possession and control of Defendants at the time of the Data Breach.

191. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

192. Plaintiff has been further injured by the damages to and diminution in value of his PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

193. Upon information and belief, Plaintiff's PII has already been stolen and misused as he has experienced incidents of fraud and identity theft in the form of fraudulent charges on his KeyBank debit card from Apple.com and foreign transaction see charges. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused great financial strain on him as a direct result of the Data Breach.

194. Furthermore, Plaintiff has experienced increased frequency of scam phone calls as a result of the Data Breach.

195. The Data Breach has also caused Plaintiff to suffer present and continuing injury arising from the substantially increased risk of additional future

fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

196. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff has spent several hours over the course of several days monitoring his financial accounts and responding to fraudulent charges on his KeyBank debit card.

197. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

198. Defendant KeyBank acknowledged the risk posed to Plaintiff and his PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years.

199. The present and continuing risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

200. Plaintiff has a continuing interest in ensuring that Plaintiff's PII, which, upon information and belief, remains backed up in Defendant's possession, is

protected, and safeguarded from future breaches.

Plaintiff M. Urciuoli's Experience

201. Plaintiff M. Urciuoli is a cautious person and is therefore very careful about sharing her sensitive PII. As a result, she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff M. Urciuoli stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff M. Urciuoli diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be.

202. Plaintiff M. Urciuoli only allowed Defendants to maintain, store, and use her PII because she believed that Defendants would use basic security measures to protect her PII, such as requiring passwords and multi-factor authentication to access databases storing her PII. As a result, Plaintiff's M. Urciuoli PII was within the possession and control of Defendants at the time of the Data Breach.

203. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff M. Urciuoli suffered injury from a loss of privacy.

204. Plaintiff M. Urciuoli has been further injured by the damages to and diminution in value of her PII—a form of intangible property that Plaintiff M. Urciuoli entrusted to Defendants. This information has inherent value that Plaintiff

M. Urciuoli was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

205. Furthermore, Plaintiff M. Urciuoli has experienced an increase in spam emails and texts, and calls as a result of the Data Breach.

206. The Data Breach has also caused Plaintiff M. Urciuoli to suffer present and continuing injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

207. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff M. Urciuoli, after learning about the Data Breach, along with her husband, Plaintiff J. Urciuoli, purchased two policies containing five (5) years of "HomeLock" home mortgage and title monitoring and protection from DomiDocs, in addition to a renewable yearly subscription of Aura identity protection. Plaintiff M. Urciuoli also froze her credit with all three credit agencies. Given that this Data Breach involved Social Security numbers, M. Urciuoli put an electronic block on her social security number and received a PIN number through the IRS for filling federal tax returns. Additionally, Plaintiff M. Urciuoli downloaded an IRS Form 14039 – Identity Theft Affidavit and faxed it to Department of the Treasury-Internal Revenue Service to alert them of the Data

Breach.

208. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff M. Urciuoli to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

209. Defendant KeyBank acknowledged the risk posed to Plaintiff M. Urciuoli and her PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years.

210. The present and continuing risk of imminent harm and loss of privacy have both caused Plaintiff M. Urciuoli to suffer stress, fear, and anxiety, including exhaustion from the emotional toll of having to take all of these actions in wake of the Data Breach.

211. Plaintiff M. Urciuoli has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff J. Urciuoli's Experience

212. Plaintiff J. Urciuoli is a cautious person and is therefore very careful

about sharing his sensitive PII. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff J. Urciuoli stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff J. Urciuoli diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

213. Plaintiff J. Urciuoli only allowed Defendants to maintain, store, and use his PII because he believed that Defendants would use basic security measures to protect his PII, such as requiring passwords and multi-factor authentication to access databases storing his PII. As a result, Plaintiff's J. Urciuoli PII was within the possession and control of Defendants at the time of the Data Breach.

214. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff J. Urciuoli suffered injury from a loss of privacy.

215. Plaintiff J. Urciuoli has been further injured by the damages to and diminution in value of his PII—a form of intangible property that Plaintiff J. Urciuoli entrusted to Defendants. This information has inherent value that Plaintiff J. Urciuoli was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

216. Furthermore, Plaintiff J. Urciuoli has experienced an increase in spam emails and texts, and calls as a result of the Data Breach.

217. The Data Breach has also caused Plaintiff J. Urciuoli to suffer present and continuing injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

218. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff J. Urciuoli, after learning about the Data Breach, along with his wife, Plaintiff M. Urciuoli, purchased two policies containing five (5) years of "HomeLock" home mortgage and title monitoring and protection from DomiDocs, in addition to a renewable yearly subscription of Aura identity protection. Plaintiff J. Urciuoli also froze his credit with all three credit agencies. Given that this Data Breach involved Social Security numbers, J. Urciuoli put an electronic block on his social security number and received a PIN number through the IRS for filling federal tax returns.

219. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff J. Urciuoli to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot

be recaptured, was spent at Defendants' direction.

220. Defendant KeyBank acknowledged the risk posed to Plaintiff J. Urciuoli and his PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years.

221. The present and continuing risk of imminent harm and loss of privacy have both caused Plaintiff J. Urciuoli to suffer stress, fear, and anxiety.

222. Plaintiff J. Urciuoli has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Patrick Reddy's Experience

223. Plaintiff Reddy is a cautious person and is therefore very careful about sharing his sensitive PII. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

224. Plaintiff Reddy only allowed Defendants to maintain, store, and use his PII because he believed that Defendants would use basic security measures to protect

his PII, such as requiring passwords and multi-factor authentication to access databases storing his PII. As a result, Plaintiff's PII was within the possession and control of Defendants at the time of the Data Breach.

225. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

226. Plaintiff has been further injured by the damages to and diminution in value of his PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

227. Upon information and belief, Plaintiff's PII has already been stolen and misused as he has experienced incidents of fraud and identity theft in the form of an unauthorized charge on his American Express account in the amount of $187.41 on or about December 8, 2022; These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused great financial strain on him as a direct result of the Data Breach.

228. Furthermore, Plaintiff has experienced a very large increase in suspicious or "spam" mailings, telephone calls, and other communications including advertisements on social media all related to his mortgage and/or finances as a result of the Data Breach.

229. The Data Breach has also caused Plaintiff to suffer present and continuing injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

230. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff has enrolled in services from Experian, Transunion and Equifax to protect his identity and credit at a total monthly expenditure of $55.

231. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice letter, time spent addressing the credit card fraud he has experienced including having to reset multiple automatic billing instructions tied to that account, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

232. Defendant KeyBank acknowledged the risk posed to Plaintiff and his PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years.

233. The present and continuing risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety.

234. Plaintiff has a continuing interest in ensuring that Plaintiff's PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Jacint "Jay" Pittman 's Experience

235. Plaintiff Pittman is a cautious person and is therefore very careful about sharing his sensitive PII. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

236. Plaintiff Pittman only allowed Defendants to maintain, store, and use his PII because he believed that Defendants would use basic security measures to protect his PII, such as requiring passwords and multi-factor authentication to access databases storing his PII. As a result, Plaintiff's PII was within the possession and control of Defendants at the time of the Data Breach.

237. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

238. Plaintiff has been further injured by the damages to and diminution in value of his PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

239. Upon information and belief, Plaintiff's PII has already been stolen and misused as he has experienced incidents of fraud and identity theft in the form of fraudulent charges to his Key Bank debit cards. As a direct result, Plaintiff Pittman spent time and effort disputing the fraudulent charges and canceling and then receiving reissued debit cards. As a result of these actions, Plaintiff believes unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused great financial strain on him as a direct result of the Data Breach.

240. Furthermore, Plaintiff has experienced additional fraudulent charges on his KeyBank debit card and wrongful activity such as spam phone calls and spam emails as a result of the Data Breach.

241. The Data Breach has also caused Plaintiff to suffer present and continuing injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

242. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff has been using paid identity theft credit monitoring subscriptions and spent time monitoring his credit and financial information.

243. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

244. Defendant KeyBank acknowledged the risk posed to Plaintiff and his PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years.

245. The present and continuing risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety as a direct result of the Data Breach.

246. Plaintiff has a continuing interest in ensuring that Plaintiff's PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiffs Joseph John Turowski, Jr.'s and Teresa Turowski's Experiences

247. Turowski Plaintiffs are cautious persons and are therefore very careful about sharing their sensitive PII. As a result, they have never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Turowski Plaintiffs store any documents containing their sensitive PII in a safe and secure location or destroys the documents. Moreover, Turowski Plaintiffs diligently choose unique usernames and passwords for their various online accounts, changing and refreshing them as needed to ensure their information is as protected as it can be.

248. Plaintiff Joseph John Turowski, Jr. and Plaintiff Teresa Turowski only allowed Defendants to maintain, store, and use their PII because they believed that Defendants would use basic security measures to protect their PII, such as requiring passwords and multi-factor authentication to access databases storing their PII. As a result, Turowski Plaintiffs' PII was within the possession and control of Defendants at the time of the Data Breach.

249. In the instant that their PII was accessed and obtained by a third party without their consent or authorization, Turowski Plaintiffs suffered injury from a loss of privacy.

250. Turowski Plaintiffs have been further injured by the damages to and diminution in value of their PII—a form of intangible property that Turowski Plaintiffs entrusted to Defendants. This information has inherent value that Turowski

Plaintiffs were deprived of when their PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

251. Furthermore, Plaintiffs veexperienced incidents of phishing phone calls and continuing phishing email spam as a result of the Data Breach.

252. The Data Breach has also caused Turowski Plaintiffs to suffer present and continuing injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from their PII being placed in the hands of criminals.

253. As a result of the actual harm they have suffered and the increased imminent risk of future harm, Plaintiffs have lost time gaining credit monitoring subscriptions and fending off phishing phone calls and continuing phishing email spam.

254. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiffs to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice letter, and self-monitoring their accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

255. Defendant KeyBank acknowledged the risk posed to Turowski

Plaintiffs and their PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years."

256. The present and continuing risk of imminent harm and loss of privacy have both caused Plaintiffs to suffer stress, fear, and anxiety.

257. Turowski Plaintiff have a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Melissa Kauffman's Experience

258. Plaintiff Melissa Kauffman is a cautious person and is therefore very careful about sharing her sensitive PII. As a result, she never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be.

259. Plaintiff Melissa Kauffman only allowed Defendants to maintain, store, and use her PII because she believed that Defendants would use basic security measures to protect her PII, such as requiring passwords and multi-factor authentication to access databases storing her PII. As a result, Plaintiff's PII was

within the possession and control of Defendants at the time of the Data Breach.

260. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

261. Plaintiff has been further injured by the damages to and diminution in value of her PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

262. Upon information and belief, Plaintiff's PII has already been stolen and misused as she has received notices indicating unknown third parties have attempted to take out loans in her name. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused great financial strain on her as a direct result of the Data Breach.

263. Furthermore, Plaintiff has experienced an increase in the number of spam emails, spam text messages, and phishing attempts as a result of the Data Breach, which has required that she expend additional time and energy combatting these new forms of spam, and defending herself against phishing attempts.

264. The Data Breach has also caused Plaintiff to suffer present and continuing injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from her PII being placed in the hands of

criminals.

265. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

266. Defendant KeyBank acknowledged the risk posed to Plaintiff and her PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years.

267. The present and continuing risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety that she will now be denied mortgage pre-approval because of the misuse of her personal information. In addition, Plaintiff has become fearful of using her accounts for online transactions.

268. Plaintiff has a continuing interest in ensuring that Plaintiff's PII, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Lebertus Vanderwerff's Experience

269. Plaintiff Vanderwerff is a cautious person and is therefore very careful

about sharing his sensitive PII. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

270. Plaintiff Vanderwerff only allowed Defendants to maintain, store, and use his PII because he believed that Defendants would use basic security measures to protect his PII, such as requiring passwords and multi-factor authentication to access databases storing his PII. As a result, Plaintiff's PII was within the possession and control of Defendants at the time of the Data Breach.

271. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

272. Plaintiff has been further injured by the damages to and diminution in value of his PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

273. Upon information and belief, Plaintiff's PII has already been stolen and misused as he has experienced incidents of fraud and identity theft in the form of

attempted purchases in his name using his credit information. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused great financial strain on him as a direct result of the Data Breach.

274. The Data Breach has also caused Plaintiff to suffer present and continuing injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

275. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendant's direction.

276. Defendant KeyBank acknowledged the risk posed to Plaintiff and his PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years.

277. The present and continuing risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety that he will have

applications for future loans, lines of credit, or other debt obligations denied because of the misuse of his personal and account information.

278. Plaintiff has a continuing interest in ensuring that Plaintiff's PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Adrianne Khanolkar's Experience

279. Plaintiff Adrianne Khanolkar is a cautious person and is therefore very careful about sharing her sensitive PII. As a result, she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts, changing and refreshing them as needed to ensure her information is as protected as it can be.

280. Plaintiff Adrianne Khanolkar only allowed Defendants to maintain, store, and use her PII because she believed that Defendants would use basic security measures to protect her PII, such as requiring passwords and multi-factor authentication to access databases storing her PII. As a result, Plaintiff's PII was within the possession and control of Defendants at the time of the Data Breach.

281. In the instant that her PII was accessed and obtained by a third party without her consent or authorization, Plaintiff suffered injury from a loss of privacy.

282. Plaintiff has been further injured by the damages to and diminution in value of her PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when her PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

283. Upon information and belief, Plaintiff's PII has already been stolen and misused as she has experienced an increase in spam text messages and phone calls as a result of the Data Breach.

284. These actions by unauthorized criminal third parties have detrimentally impacted Plaintiff's life as a whole, and specifically caused great financial distress on her as a direct result of the Data Breach because the criminals now have all but one of the digits in her social security number, which places her at present and continuing injury arising from the substantially increased risk of future fraud, identity theft, and misuse resulting from her PII being placed in the hands of criminals.

285. As a result of the actual harm she has suffered and the increased imminent risk of future harm, Plaintiff spent about 3 hours requesting credit reports from each credit bureau and requesting a credit freeze.

286. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to

the Data Breach, which includes time spent verifying the legitimacy of the Notice letter, and self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

287. Defendant KeyBank acknowledged the risk posed to Plaintiff and her PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years.

288. The present and continuing risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, and anxiety. Plaintiff has anxiety due to her personal information being on the internet forever, especially because the criminals now have all but one of the digits in her social security number, and she will always feel like she is at risk of identity theft.

289. Plaintiff has a continuing interest in ensuring that Plaintiff's PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Dharmendra Khanolkar's Experience

290. Plaintiff Dharmendra Khanolkar is a cautious person and is therefore very careful about sharing his sensitive PII. As a result, he never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured

source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

291. Plaintiff Dharmendra Khanolkar only allowed Defendants to maintain, store, and use his PII because he believed that Defendants would use basic security measures to protect his PII, such as requiring passwords and multi-factor authentication to access databases storing his PII. As a result, Plaintiff's PII was within the possession and control of Defendants at the time of the Data Breach.

292. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

293. Plaintiff has been further injured by the damages to and diminution in value of his PII—a form of intangible property that Plaintiff entrusted to Defendant. This information has inherent value that Plaintiff was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

294. Upon information and belief, Plaintiff's PII has already been stolen and misused as he has experienced an increase in spam text messages and phone calls as a result of the Data Breach.

295. These actions by unauthorized criminal third parties have detrimentally

impacted Plaintiff's life as a whole, and specifically caused great financial distress on him as a direct result of the Data Breach because the criminals now have all but one of the digits in his social security number, which places him at present and continuing injury arising from the substantially increased risk of future fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

296. The Data Breach has also caused Plaintiff to suffer present and continuing injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

297. As a result of the actual harm he has suffered and the increased imminent risk of future harm, Plaintiff spent time assisting his wife with reviewing their credit reports and reviewing monthly statements for fraudulent activity.

298. In addition to the increased risk and the actual harm suffered, the Data Breach has caused Plaintiff to spend significant time dealing with issues related to the Data Breach, which includes time spent verifying the legitimacy of the Notice letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time, which has been lost forever and cannot be recaptured, was spent at Defendants' direction.

299. Defendant KeyBank acknowledged the risk posed to Plaintiff and his

PII, both by explicitly stating that "keeping [its customers'] personal information safe and secure is of utmost importance to us" and by offering temporary complimentary monitoring for two years.

300. The present and continuing risk of imminent harm and loss of privacy have both caused Plaintiff to suffer stress, fear, anxiety, and annoyance.

301. Plaintiff has a continuing interest in ensuring that Plaintiff's PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff Joynequa West's Experience

302. Plaintiff West was required to provide and did provide her sensitive PII to OSC during her banking relationship with Fulton Bank.

303. To date, OSC has done next to nothing to adequately protect Plaintiff or to compensate her for their injuries sustained in this Data Breach particularly given the fact that the unencrypted PII has already been exfiltrated and likely made available to anyone wishing to download it.

304. Defendant OSC's notice letter downplays the theft of Plaintiff's PII, when the facts demonstrate that the PII was deliberately exfiltrated in a criminal action.

305. The fraud and identity monitoring services offered by Defendant OSC are only for two years, and Defendant OSC places the burden squarely on Plaintiff

by requiring her to expend time signing up for the service and addressing timely issues resulting from the Data Breach.

306. Plaintiff West has been further damaged by the compromise of her PII.

307. Plaintiff West's PII was compromised in the Data Breach and was likely stolen and in the hands of cybercriminals who targeted and illegally accessed Defendant OSC's network for the specific purpose of targeting the PII.

308. Plaintiff typically takes measures to protect her PII and is very careful about sharing her PII. Plaintiff has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

309. Plaintiff stores any documents containing her PII in a safe and secure location, and she diligently chooses unique usernames and passwords for her online accounts.

310. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. In response to the Data Breach, Plaintiff has spent significant time monitoring her accounts and credit score and has sustained emotional distress in addition to her lost time. This is time that was lost and unproductive and took away from other activities and duties.

311. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her PII —a form of intangible property that she entrusted

to Defendant OSC for the purpose of obtaining services from Fulton Bank, which was compromised in and as a result of the Data Breach.

312. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

313. Plaintiff has suffered present and continuing injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of criminals.

314. Defendants OSC obtained and continue to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Fulton Bank required the PII from Plaintiff when she received services from OSC. Plaintiff, however, would not have entrusted her PII to OSC, or allowed OSC to retain her PII, had she known that it would fail to maintain adequate data security. Plaintiff's PII was compromised, disclosed, and stolen as a result of the Data Breach.

315. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

316. Plaintiff has a continuing interest in ensuring that her PII, which upon information and belief, remains in OSC's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

317. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

318. The Nationwide Class that Plaintiffs seek to represent is preliminarily defined as follows:

> All individuals whose PII was compromised in the data breach that is the subject of the Notice of Vendor Security Incident that KeyBank and others sent to Plaintiffs and Class Members on or around August 26, 2022 (the "Nationwide Class").

319. In addition to the Nationwide Class, Plaintiffs and Class Members seek to represent the following subclasses.

320. Plaintiffs Mariann Archer, Mark Samsel, Tim Marlowe, Melissa Urciuoli, James Urciuoli, Patrick Reddy, Jacint "Jay" Pittman, Joseph John Turowski, Jr., Teresa Turowski, Melissa D. Kauffman, Lebertus Vanderwerff, Adrianne Khanolkar, and Dhamendra "DK" Khanolkar ("Contract Plaintiffs") seek to represent a class of persons who provided their PII to KeyBank preliminarily defined as follows:

> All individuals who provider their PII to KeyBank and whose PII was compromised in the data breach that is the subject of the Notice of Vendor Security Incident that KeyBank and others sent to Plaintiffs and Class Members on or around August 26, 2022 (the "Contract Class").

321. Plaintiffs Dhamendra "DK" Khanolkar and Adrianne Khanolkar ("California Plaintiffs") seek to represent a class of California residents preliminarily defined as follows:

> All individuals who reside in the state of California and whose PII was compromised in the data breach that is the subject of the Notice of Vendor Security Incident that KeyBank and others sent to Plaintiffs and Class Members on or around August 26, 2022 (the "California Class").

322. Plaintiffs Mariann Archer and Lebertus Vanderwerff ("New York Plaintiffs") seek to represent a class of New York residents preliminarily defined as follows:

> All individuals who reside in the state of New York and whose PII was compromised in the data breach that is the subject of the Notice of Vendor Security Incident that KeyBank and others sent to Plaintiffs and Class Members on or around August 26, 2022 (the "New York Class").

323. Plaintiffs James Urciuoli and Melissa Urciuoli ("Oregon Plaintiffs") seek to represent a class of Oregon residents preliminarily defined as follows:

> All individuals who reside in the state of Oregon and whose PII was compromised in the data breach that is the subject of the Notice of Vendor Security Incident that KeyBank and others sent to Plaintiffs and Class Members on or around August 26, 2022 (the "Oregon Class").

324. Plaintiffs Joynequa West, Jacint Pittman, Joseph John Turowski, Jr., and Teresa Turowski ("Pennsylvania Plaintiffs") seek to represent a class of Pennsylvania residents preliminarily defined as follows:

> All individuals who reside in the state of Pennsylvania and whose PII was compromised in the data breach that is the subject of the Notice of Vendor Security Incident that KeyBank and others sent to Plaintiffs and Class Members on or around August 26, 2022 (the "Pennsylvania Class").

325. Plaintiff Patrick Reddy ("Washington Plaintiff") seeks to represent a class of Washington residents preliminarily defined as follows:

> All individuals who reside in the state of Washington and whose PII was compromised in the data breach that is the subject of the Notice of Vendor Security Incident that KeyBank and others sent to Plaintiffs and Class Members on or around August 26, 2022 (the "Washington Class").

326. Excluded from the Class and Subclasses are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

327. Plaintiffs reserve the right to modify or amend the definition of the

proposed classes before the Court determines whether certification is appropriate.

328. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendants have identified thousands of individuals whose PII was compromised in the Data Breach, and the Class is apparently identifiable within Defendants' records. KeyBank notified the Attorney General of Massachusetts that 4,588 Massachusetts residents were affected by the Data Breach and notified the Attorney General of Montana that 228 Montana residents were affected by the Data Breach.

329. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendants had duties to protect the PII of Plaintiffs and Class Members;

b. Whether Defendants had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendants had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiffs and Class Members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;

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

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

330. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of

those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

331. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

332. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

333. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims

involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

334. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions

would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

335. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

336. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

337. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

338. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

339. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed legal duties to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duties to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between KeyBank on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether KeyBank breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;

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

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class

Members; and,

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class against each Defendant)

340. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

341. Plaintiffs and Class Members were required to submit non-public PII as a condition of obtaining products and/or services from Defendants and/or one of Defendants' client companies.

342. Plaintiff and the Class Members entrusted their PII to Defendants with the understanding that Defendants would safeguard their information and delete it once it was no longer required to retain it after the end of the consumer relationship.

343. Defendants had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members.

344. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 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.

345. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

346. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

347. Defendants' 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 Defendants are bound by industry standards to protect confidential PII.

348. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

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

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

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

d. Allowing unauthorized access to Class Members' PII.

349. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the industry.

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

351. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored in an Internet-accessible environment.

352. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

353. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendants' possession.

354. Defendants were in an exclusive position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

355. There is a temporal and close causal connection between Defendants' failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiffs and the Class.

356. As a result of Defendants' negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: (i) lost or diminished value of PII; (ii) invasion of privacy; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendants' possession and is subject to further

unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

357. Plaintiffs and Class Members are entitled to nominal, compensatory, and consequential damages suffered as a result of the Data Breach as well as any other relief allowed by law.

358. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants 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) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Negligence *per se*
(On Behalf of Plaintiffs and the Nationwide Class against each Defendant)

359. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

360. Plaintiff and the Class Members entrusted their PII to Defendants with the understanding that Defendants would safeguard their information and delete it once it was no longer required to retain it after the end of the consumer relationship.

361. Defendants had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiff and Class Members.

362. Defendants had a duty to employ reasonable security measures under

Section 5 of the Federal Trade Commission Act, 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.

363. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 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.

364. Defendants' duty to use reasonable security measures also arose under the GLBA, under which Defendants were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

365. Plaintiffs and Class Members were within the Class of Persons the GLBA and the FTC Act were intended to protect and the consequences of the Data Breach are the types of harm against which the statutes were intended to protect.

366. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the

following:

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

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

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

d. Allowing unauthorized access to Class Members' PII.

367. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the industry.

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

369. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored in an Internet-accessible environment.

370. As a result of Defendants' negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: (i) lost or diminished value of PII; (ii) invasion of privacy; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

371. Plaintiffs and Class Members are entitled to nominal, compensatory, and consequential damages suffered as a result of the Data Breach as well as any other relief allowed by law.

372. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants 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) continue to provide adequate credit monitoring to all Class Members.

COUNT III
Breach of Contract
(On Behalf of Contract Plaintiffs and the Contract Class against Defendant KeyBank)

373. Contract Plaintiffs ("Plaintiffs" for the purposes of this Count) re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

374. KeyBank's Online Banking Service Agreement and Disclosure which controls and supersedes any agreements between KeyBank and its customers, expressly provides that "[KeyBank] will protect and share your information as described in the KeyCorp Privacy Notice."[39]

375. In the KeyBank Privacy Notice, KeyBank represents that, "[t]o protect your information from unauthorized access and use, we use security measures that comply with federal law. These measures includes computer safeguards and secured files and buildings."

376. In being residential mortgage clients of KeyBank, Plaintiffs and the Nationwide Class provided and entrusted their PII to KeyBank and agreed to and adhered by KeyBank's Online Banking Service Agreement and Disclosure and the KeyBank Privacy Notice, which, on information and belief, is provided to all of KeyBank's customers.

[39] https://www.key.com/personal/online-banking/online-banking-service-agreement-disclosure.html

377. KeyBank's public representations and conduct, including those made in its privacy policies and marketing statements, confirm that KeyBank bound and obligated itself to protect the PII that Plaintiffs and the Contract Class submitted to KeyBank.

378. KeyBank required Plaintiffs and the Contract Class to provide and entrust to it their PII as condition of their respective financial transactions with KeyBank. In return, KeyBank promised to "use security measures that comply with federal law [including] computer safeguards and secured files and buildings."

379. As a condition of being past and current clients of KeyBank, Plaintiffs and the Contract Class provided and entrusted their PII to KeyBank. In so doing, Plaintiffs and the Contract Class entered into contracts with KeyBank by which KeyBank agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiffs and the Contract Class if their PII had been compromised or stolen.

380. Plaintiffs and the Contract Class fully performed their obligations under the contracts with KeyBank.

381. KeyBank breached the contracts it made with Plaintiffs and the Contract Class by (i) failing to encrypt Plaintiffs' and the Contract Class's PII before sharing it with OSC and (ii) failing to ensure that OSC encrypted the PII while storing it in an Internet-accessible environment, and (iii) failing to ensure that OSC

otherwise safeguarded and protected the PII.

382. As a direct and proximate result of KeyBank's above-described breach of contract, Plaintiffs and the Contract Class have suffered (and will continue to suffer) the lost benefit of the bargains they struck with KeyBank, the threat of the sharing and detrimental use of their sensitive information; ongoing, current and continuing threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

383. As a direct and proximate result of KeyBank's breach of contract, Plaintiffs and the Contract Class are entitled to recover actual, compensatory, consequential, and nominal damages as well as any other relief allowed by law.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class against each Defendant)

384. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

385. Contract Plaintiffs plead this count in the alternative to Count II above.

386. When Plaintiffs and Class Members paid for services and provided their PII to the entities that entrusted it to OSC, they did so on the mutual understanding and expectation that OSC would use a portion of those payments, or revenue derived from the use of their PII, to adequately fund data security practices.

387. Upon information and belief, OSC funds their data security measures entirely from their general revenues, including payments made by or on behalf of Plaintiffs and Class Members and revenue derived from the PII provided by Plaintiffs and Class Members.

388. Upon information and belief, KeyBank funds their data security measures entirely from their general revenues, including payments made by or on behalf of Plaintiffs and Class Members and revenue derived from the PII provided by Plaintiffs and Class Members.

389. As such, a portion of the payments made by or on behalf of Plaintiffs and Class Members, or the revenue derived from their PII, is to be used by Defendants to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

390. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class

Members' PII and instead directing those funds to their own profits. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security.

391. Defendants knew that Plaintiffs and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used the PII of Plaintiffs and Class Members for business purposes.

392. For years and continuing to today, Defendants' business models have depended upon their use of consumers' PII. Trust and confidence are critical and central to the services provided by Defendants in the financial industry. Unbeknownst to Plaintiffs and absent Class Members, however, Defendants did not secure, safeguard, or protect its customers' and employees' data and employed deficient security procedures and protocols to prevent unauthorized access to customers' PII. Defendants' deficiencies described herein were contrary to their security messaging.

393. Plaintiffs and Class Members received services from Defendants, and Defendants were provided with, and allowed to collect and store, their PII on the

mistaken belief that Defendants complied with their duties to safeguard and protect its customers' and employees' PII.

394. Upon information and belief, putting their short-term profit ahead of safeguarding PII, and unbeknownst to Plaintiffs and Class Members, Defendants knowingly sacrificed data security to save money at their expense and to their detriment.

395. Upon information and belief, Defendants knew that the manner in which they maintained and transmitted customer PII violated industry standards and their fundamental duties to Plaintiffs and Class Members by neglecting well accepted security measures to ensure confidential information was not accessible to unauthorized access. Defendants had knowledge of methods for designing safeguards against unauthorized access and eliminating the threat of exploit, but it did not use such methods.

396. Defendants had within their exclusive knowledge, and never disclosed, that they had failed to safeguard and protect Plaintiffs and Class Members' PII. This information was not available to Plaintiffs, Class Members, or the public at large.

397. Defendants also knew that Plaintiffs and Class Members expected security against known risks and that they were required to adhere to state and federal standards for the protection of confidential personally identifying, financial, and other personal information.

398. Plaintiffs and Class Members did not expect that Defendants would knowingly insecurely maintain and hold their PII when that data was no longer needed to facilitate a business transaction or other legitimate business reason. Likewise, Plaintiffs and Class Members did not know or expect that Defendants would employ substantially deficient data security systems and fail to undertake any required monitoring or supervision of the entrusted PII.

399. Had Plaintiffs and Class Members known about Defendants' deficiencies and efforts to hide their ineffective and substandard data security systems, Plaintiffs and Class Members would not have entered into business dealings with Defendants.

400. By withholding the facts concerning the defective security and protection of customer PII, Defendants put their own interests ahead of the very customers who placed their trust and confidence in Defendants and benefitted themselves to the detriment of Plaintiffs and Class Members.

401. It would be inequitable, unfair, and unjust for Defendants to retain these wrongfully obtained fees and benefits. Defendants' retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

402. Plaintiffs and Nationwide Class Members have no adequate remedy at law.

403. Plaintiffs and each Member of the proposed Class are each entitled to restitution and non-restitutionary disgorgement in the amount by which Defendants were unjustly enriched, to be determined at trial.

COUNT V
Violation of the Georgia Uniform Deceptive Trade Practices Act, Ga. Code Ann. §§ 10-1-370, *et seq*
(On Behalf of Plaintiffs and the Nationwide Class against each Defendant)

404. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

405. OSC, KeyBank, Plaintiffs, and Class Members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

406. OSC and KeyBank engaged in deceptive trade practices in the conduct of their business, in violation of Ga. Code § 110-1-372(a), including:

e. Representing that goods or services have characteristics that they do not have;

f. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

g. Advertising goods or services with intent not to sell them as advertised;

h. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

2. OSC's and KeyBank's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' PII, 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 following previous cybersecurity incidents, 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 Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that Defendants would protect the privacy and confidentiality of Plaintiffs' and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that Defendants would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiffs' and Class members' PII; and

g. Omitting, suppressing, and concealing the material facts that Defendants did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

407. OSC's and KeyBank's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Personal Information.

408. Defendants intended to mislead Plaintiff and Class Members and induce them to rely on their misrepresentations and omissions.

409. In the course of its business, Defendants engaged in activities with a tendency or capacity to deceive.

410. Defendants acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiffs and Class members' rights. Breaches within the financial industry put Defendants on notice that its security and privacy protections were inadequate.

411. Had OSC and KeyBank disclosed to Plaintiffs and Class Members that OSC's data systems were not secure and, thus, vulnerable to attack, OSC 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, OSC and KeyBank received, maintained, and compiled Plaintiffs' and Class Members' PII as part of the services OSC provided and for which Plaintiffs and class members paid without advising Plaintiffs and class members that OSC's data security practices were insufficient to maintain the safety and confidentiality of Plaintiffs' and Class Members' PII. Accordingly, Plaintiffs and the Class members acted reasonably in relying on OSC's and KeyBank's misrepresentations and omissions, the truth of which they could not have discovered.

412. As a direct and proximate result of OSC's deceptive trade practices, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with OSC and KeyBank, as they would not have paid OSC and KeyBank for goods and services or would have paid less for such goods and services but for OSC's and KeyBank's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased,

imminent risk of fraud and identity theft.

413. Plaintiffs and Class Members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under Ga. Code § 10-1-373.

COUNT VI
Violation of California's Unfair Competition Law ("UCL")
(On Behalf of California Plaintiffs and the California Class against each Defendant)

414. Plaintiffs Dhamendra "DK" Khanolkar, Adrianne Khanolkar ("Plaintiffs" for the purposes of this Count) and the California Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

415. The UCL prohibits any "unlawful" or "unfair" business act or practice, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful and unfair practices within the meaning, and in violation, of the UCL.

416. In the course of conducting its business, Defendants committed "unlawful" business practices by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and California Class Members'

PII, and by violating the statutory and common law alleged herein, including, inter alia, the Graham Leach Bliley Act Privacy Rule, 16 C.F.R. Part 313, and Reg. P, 12 C.F.R. Part 1016 and Section 5 of the FTC Act. Plaintiffs and California Class members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

417. Defendants also violated the UCL by failing to timely notify Plaintiffs and California Class members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiffs and California Class members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

418. Defendants also violated the UCL by failing to abide by its posted privacy policy.

419. Defendants violated the unfair prong of the UCL by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Class Members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and California Class Members' PII in an unsecure electronic environment.

420. These unfair acts and practices were immoral, unethical, oppressive,

unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and California Class members. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiffs and California Class members outweighed their utility, if any.

421. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral, unethical, oppressive, and unscrupulous.

422. Defendants' practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the GLBA, California's California Consumer Privacy Act and Confidentiality of Medical Information Act, and the FTC Act (15 U.S.C. § 45). The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

423. Plaintiffs and California Class Members suffered injury in fact and lost

money or property as a result of Defendants' violations of statutory and common law. Plaintiffs and the California Class suffered from overpaying for services that should have included adequate data security for their PII, by experiencing a diminution of value in their PII as a result if its theft by cybercriminals, the loss of Plaintiffs' and California Class Members' legally protected interest in the confidentiality and privacy of their PII, the right to control that information, and additional losses as described above.

424. Plaintiffs and California Class Members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia, (i) an imminent, immediate and the continuing increased risk of identity theft and identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) deprivation of the value of their PII for which there is a well-established national and international market, and/or (v) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

425. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. As such, Plaintiffs Dhamendra "DK" Khanolkar and Adrianne Khanolkar, on behalf of themselves and California Class Members, seek restitution and an injunction,

including public injunctive relief prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203. To the extent any of these remedies are equitable, Plaintiffs Dhamendra "DK" Khanolkar, Adrianne Khanolkar and the Class seek them in the alternative to any adequate remedy at law they may have.

COUNT VII
Violation of New York's General Business Law § 349, *et seq*.
(On Behalf of New York Plaintiffs and the New York Class against Each Defendant)

426. Plaintiffs Mariann Archer and Lebertus Vanderwerff ("Plaintiffs" for the purposes of this Count) and the New York Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

427. Defendants engaged in deceptive acts or practices in the conduct of their business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members PII, which was a proximate and direct 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 following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII, including by implementing and maintaining reasonable security measures;

d. Failing to timely and adequately notify the Plaintiffs and Class Members of the Data Breach;

e. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Class Members' PII; and

f. 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 Class Members' PII, including duties imposed by the FTC Act and the Graham Leach Bliley Act.

428. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' PII.

429. Defendants' representations and omissions were material because they

were likely to deceive reasonable consumers.

430. Defendants acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiffs' and New York Class Members' rights.

431. As a direct and proximate result of Defendants' deceptive and unlawful acts and practices, Plaintiff and New York Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

432. Defendants' conduct is unconscionable, deceptive, and unfair, and is substantially likely to and did mislead consumers such as Plaintiffs and the New York Class acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiffs and the Class have been injured because they were not timely notified of the Data Breach causing their PII to be comprised.

433. Defendants' deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large.

434. The above deceptive and unlawful practices and acts by Defendants caused substantial injury to Plaintiffs and Class Members that they could not reasonably avoid.

435. Plaintiffs Mariann Archer and Lebertus Vanderwerff and New York Class Members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

COUNT VIII
Violation of Oregon's Unfair Trade Practices Act
(On Behalf of Oregon Plaintiffs and the Oregon Class against each Defendant)

436. Plaintiffs James Urciuoli and Melissa Urciuoli ("Plaintiffs" for the purposes of this Count) and the Oregon Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

437. Plaintiffs James Urciuoli and Melissa Urciuoli bring this Count on their own behalf and that of the Oregon Class for violations of the Oregon Unfair Trade Practices Act, Or. Rev. Stat. § 646.608(1)€(g) and (u), et seq.

438. Defendants engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale, performance, and advertisement of their services, including: (1) failing to maintain adequate data security to keep Plaintiffs' and the Oregon Class's sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (2) failing to disclose or omitting materials facts to Plaintiffs and the Oregon Class regarding their lack of adequate data security and inability or

unwillingness to properly secure and protect the PII of Plaintiffs and the Oregon Class; (3) failing to disclose or omitting material facts to Plaintiffs and the Oregon Class about Defendants' failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiffs; and (4) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiffs' and the Oregon Class's PII and other personal information from further unauthorized disclosure, release, data breaches, and theft.

439. Defendant KeyBank failed to properly audit, supervise, or ensure that OSC's data security practices were adequate in light of the volume and sensitivity of information that it allowed OSC to maintain.

440. These actions also constitute deceptive and unfair acts or practices because Defendants knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiffs James Urciuoli and Melissa Urciuoli and the Oregon Class and defeat their reasonable expectations about the security of their PII.

441. Moreover, Defendants each represented that they would maintain the data it collected and custodied in a secure manner and endeavor to keep it safe from unauthorized access and exfiltration.

442. Defendants intended that Plaintiffs James Urciuoli and Melissa Urciuoli and the Oregon Class rely on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's offering of goods and services.

443. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendants' generalized course of conduct that applied to the Oregon Class. Plaintiffs James Urciuoli and Melissa Urciuoli and the Oregon Class have been adversely affected by Defendants' conduct and the public was and is at risk as a result thereof.

444. Defendants also violated Or. Rev. Stat. Ann. § 646A.604(1), et seq. by failing to immediately notify Plaintiffs James Urciuoli and Melissa Urciuoli and the Oregon Class of the nature and extent of the Data Breach.

445. As a result of Defendants' wrongful conduct, Plaintiffs James Urciuoli and Melissa Urciuoli and the Oregon Class were injured in that they never would have provided their PII to Defendant, or purchased Defendant's services, had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

446. As a direct and proximate result of Defendant's violations described herein, Plaintiffs James Urciuoli and Melissa Urciuoli and the Oregon Class have suffered harm, including actual instances of identity theft; loss of time and money

resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the payments or services made to Defendant or Defendant's customers that Plaintiffs James Urciuoli and Melissa Urciuoli and the Oregon Class would not have made had they known of Defendant's inadequate data security; lost control over the value of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

447. Plaintiffs James Urciuoli and Melissa Urciuoli and the Oregon Class seek actual and compensatory damages, injunctive relief, statutory damages, and court costs and attorneys' fees as a result of Defendants' violations of Oregon's consumer protection statutes.

COUNT IX
Violation of Pennsylvania's Unfair Trade Practices Act
(On Behalf of Pennsylvania Plaintiffs and the Pennsylvania Class against each Defendant)

448. Plaintiffs Joynequa West, Jacint Pittman, Jospeh John Turowski, Jr., and Teresa Turowski ("Plaintiffs" for the purposes of this Count) and the Pennsylvania Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

449. As a consumer of Defendants' services, directly or indirectly, Plaintiffs

are authorized to bring a private action under Pennsylvania's Unfair Trade Practices and Consumer Protection Law ("UTPCPL"). 73 P.S. § 201-9.2.

450. Plaintiffs are "a person" within the meaning of 73 P.S. § 201-2(2).

451. Plaintiffs and Class Members provided their PII to Defendants pursuant to transactions in "trade" and "commerce" as meant by 73 P.S. §201-2(3), for personal, family, and/or household purposes.

452. The UTPCPL prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce".]" 73 P.S. § 201-3.

453. This Count is brought for Defendants' unfair and deceptive conduct, including Defendants' unlawful and unfair and deceptive acts and practices, which "creat[ed] a likelihood of confusion or of misunderstanding" for Plaintiffs and Class Members as meant by 73 P.S. § 201-2(4)(xxi).

454. Defendants engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale and advertisement of the goods purchased by Plaintiffs and the Class in violationof 73 P.S. § 201-3, including but not limited to the following:

h. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members PII, which was a proximate and direct cause of the Data Breach;

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

j. Misrepresenting that they would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII, including by implementing and maintaining reasonable security measures;

k. Failing to timely and adequately notify the Plaintiffs and Class Members of the Data Breach;

l. Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff and Class Members' PII; and

m. 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 Class Members' PII, including duties imposed by the FTC Act and the Graham Leach Bliley Act.

455. The above unfair and deceptive acts and practices by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to consumers that the consumers could not reasonably avoid. This substantial

injury outweighed any benefits to consumers or to competition.

456. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiffs and Class Memb'rs' PII and that the risk of a data breach or theft was highly likely. Defendants actions in engaging in the above-named deceptive acts and practices were negligent, knowing, and reckless with respect to the rights of Plaintiffs and Class Members.

457. Plaintiffs and Class Members relied on Defendants' unfair and deceptive acts and practices when they paid money in exchange for goods and services and provided their PII to KeyBank, and by extension to OSC.

458. Plaintiffs and Class Members relied on Defendants to safeguard and protect their PII and to timely and accurately notify them if their data had been breached and compromised.

459. Plaintiffs and Class Members would not have paid for Defendants services, or would have paid less, had they known that Defendants did not implement reasonable data security policies and procedures.

460. Plaintiffs and Class Members seek all available relief under the UTPCPL, 73 P.S. § 201-1 et seq.

COUNT X
Violation of the Washington Consumer Protection Act
(On Behalf of Washington Plaintiffs and the Washington Class against each Defendant)

461. Plaintiff Patrick Reddy ("Plaintiff" for the purposes of this Count) and

the Washington Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

462. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

463. Defendants are a "person" as described in RWC 19.86.010(1).

464. Defendants engage in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

465. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendants engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendants' practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

466. In the course of conducting their business, Defendants committed "unfair or deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' PII, and

violating the common law alleged herein in the process. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendants constituting other unlawful business acts or practices. As described above, Defendants' wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

467. Defendants also violated the CPA by failing to timely notify and concealing from Plaintiffs and Class Members information regarding the unauthorized release and disclosure of their PII. If Plaintiffs and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their PII, medical information, and identities.

468. Defendants' above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendants' wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

469. The gravity of Defendants' wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

470. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the CPA, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud and medical fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their PII; (5) deprivation of the value of their PII, for which there is a well-established national and legitimate market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

471. Unless restrained and enjoined, Defendants will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff Reddy, therefore, on behalf of himself and the Class, seeks restitution and an injunction prohibiting Defendants from continuing such wrongful conduct, and requiring Defendants to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to them.

472. Plaintiff Reddy, on behalf of himself and Class Members, also seeks to

recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiff Reddy, on behalf of himself and Class Members, request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained not to exceed $25,000.00 per Class Member.

COUNT XI
Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*
(On Behalf of Plaintiffs and the Nationwide Class against each Defendant)

473. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

474. Plaintiffs bring this Count on behalf of themselves and on behalf of the Nationwide Class.

475. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

476. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs

and the Nationwide Class allege that Defendants' data security measures remain inadequate. Defendants publicly deny these allegations. Furthermore, Plaintiffs and the Nationwide Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendants have undertaken in response to the Data Breach.

477. Plaintiffs and the Nationwide Class have an ongoing, actionable dispute arising out of Defendants' inadequate security measures, including (i) Defendants' failure to encrypt Plaintiffs' and the Nationwide Class's PII, including driver's license numbers, while storing it in an Internet-accessible environment and (ii) Defendants' failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the driver's license number of Plaintiffs and the Nationwide Class.

478. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendants owe a legal duty to secure the PII that they continue to maintain;

b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

c. Defendants' ongoing breaches of their legal duty continue to cause Plaintiffs and the Nationwide Class harm.

479. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendants to:

a. engage third party auditors, consistent with industry standards, to test their systems for weakness and upgrade any such weakness found;

b. audit, test, and train their data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test their systems for security vulnerabilities, consistent with industry standards; and

d. implement an education and training program for appropriate employees regarding cybersecurity.

480. If an injunction is not issued, Plaintiffs and the Nationwide Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiffs and the Nationwide Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify

the same conduct.

481. The hardship to Plaintiffs and the Nationwide Class if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiffs and the Nationwide Class will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

482. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiffs and the Nationwide Class and others whose confidential information would be further compromised.

COUNT XII
Recovery of Expenses of Litigation, O.C.G.A. § 13-6-11 (On Behalf of Plaintiffs and the Nationwide Class against each Defendant)

483. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 339.

484. Pursuant to O.C.G.A. § 13-6-11, the jury may allow the expenses of litigation and attorneys' fees as part of the damages where a defendant "has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary

trouble and expense."

485. Defendants through their actions alleged and described herein acted in bad faith, were stubbornly litigious, or caused the Plaintiffs and the Class Members unnecessary trouble and expense with respect to the transaction or events underlying this litigation.

486. The Plaintiffs and the Class Members request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Nationwide Class and Subclasses and appointing Plaintiffs and their Counsel to represent such Class and Subclasses;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendants to protect, including through encryption, all data collected through the course of their business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;

v. prohibiting Defendants from maintaining the PII of Plaintiffs and

Class Members on a cloud-based database;

vi. requiring Defendants to engage independent 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;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of OSC network is compromised, hackers cannot gain access to other portions of OSC's systems;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training

for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor OSC's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from OSC's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, pursuant to O.C.G.A. § 13-6-11 and as otherwise allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: June 12, 2023

Respectfully Submitted,

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
The Finley Firm, P.C.
Building 14, Suite 230
3535 Piedmont Road
Atlanta, GA 30305
Phone: 404-320-9979
Fax: 404-320-9978
Email: mgibson@thefinleyfirm.com

John A. Yanchunis
Ryan D. Maxey
Morgan & Morgan Complex Litigation Group
201 N. Franklin Street
Tampa, FL 33602
813-223-5505
Fax: 813-222-2434
Email: jyanchunis@forthepeople.com
Email: rmaxey@forthepeople.com

Jared William Connors
Matthew Ryan Wilson
Michael Joseph Boyle , Jr.
Meyer Wilson Co., LPA
305 W. Nationwide Blvd.
Columbus, OH 43215
630-224-6000
Email: jconnors@meyerwilson.com
Email: mwilson@meyerwilson.com
Email: mboyle@meyerwilson.com

Raina C Borrelli
Samuel J. Strauss
Turke & Strauss, LLP -WI
613 Williamson Street, Suite 201
Madison, WI 53703

608-237-1775
Fax: 608-509-4423
Email: raina@turkestrauss.com
Email: sam@turkestrauss.com

Charles E. Schaffer
Levin Sedran & Berman
510 Walnut Street, Suite 500
Philadelphia, PA 19106-3697
215-592-1500
Fax: 215-592-4663
Email: cschaffer@lfsblaw.com

Gregory John Bosseler
Morgan & Morgan, PLLC
178 S. Main Street, Suite 300
Alpharetta, GA 30049 239-433-6880
Email: gbosseler@forthepeople.com

Jeffrey Goldenberg
Goldenberg Schneider, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
513-345-8291
Email: jgoldenberg@gs-legal.com

Kyle G.A. Wallace
Shiver Hamilton Campbell LLC
3490 Piedmont Road Suite 640
Atlanta, GA 30305
404-593-0020
Fax: 888-501-9536
Email: kwallace@shiverhamilton.com

Michael Anderson Berry
Gregory Haroutunian
Arnold Law Firm
865 Howe Avenue
Sacramento, CA 95825
916-239-4787

Email: aberry@justice4you.com
Email: gharoutunian@justice4you.com

Terence R. Coates
Markovits, Stock & Demarco, LLC
119 E. Court Street, Suite 530
Cincinnati, OH 45202
513-651-3700
Fax: 513-665-0219
Email: tcoates@msdlegal.com

Alfred G. Yates , Jr.
Law Office of Alfred G. Yates, Jr., P.C.
1575 McFarland Road Ste 305
Pittsburgh, PA 15216
412-391-5164
Email: yateslaw@aol.com

Joseph P. Guglielmo
Carey Alexander
Scott & Scott, LLP-NY
17th Floor, 230 Park Avenue
New York, NY 10169
212-223-6444
Fax: 212-223-6334
Email: jguglielmo@scott-scott.com
Email: calexander@scott-scott.com

Mark Edward Dann
Brian D. Flick
Dann Law Firm
15000 Madison Avenue
Lakewood, OH 44107
216-373-0539
Fax: 216-373-0536
Email: notices@dannlaw.com

Thomas A. Zimmerman, Jr.
Thomas A. Zimmerman, Jr. Attorney at Law

77 W. Washington Street Suite 1220
Chicago, IL 60602
312-440-0020
Email: tom@attorneyzim.com

Gary F. Lynch
Lynch Carpenter, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
412-322-9243
Email: Gary@lcllp.com

Amanda Grace Fiorilla
Lowey Dannenberg, P.C.
44 South Broadway, Suite 1100
White Plains, NY 10601
914-733-7266
Email: afiorilla@lowey.com

Anthony Christina
Lowey Dannenberg, P.C.
One Tower Bridge
100 Front Street, Suite 520
19428
West Conshohocken, PA 19081
215-399-4770
Email: achristina@lowey.com

Christian Levis
Lowey Dannenberg, P.C. - NY
44 South Broadway Suite 1100
White Plains, NY 10601
914-997-0500
Fax: 914-997-0035
Email: clevis@lowey.com

James J. Pizzirusso
Hausfeld LLP
888 16th Street, Ste 300
Washington, DC 20006

202-540-7200
Email: jpizzirusso@hausfeld.com

Mark Abramowitz
DiCello Levitt and Casey LLC
7556 Mentor Avenue
Mentor, OH 44060
440-953-8888
Email: marka@dicellolaw.com

Amy E. Keller
DICELLO LEVITT LLC
Ten North Dearborn Street
Sixth Floor
Chicago, Illinois 60602
Tel: 312-241-7900
Email: akeller@dicellolevitt.com

Steven Nathan
Hausfeld, LLP
33 Whitehall Street
New York, NY 10004
646-357-1194
Fax: 212-202-4322
Email: snathan@hausfeld.com

Gary M. Klinger
Milberg Coleman Bryson Phillips Grossman PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
866-252-0878
Email: gklinger@milberg.com

David K. Lietz
Milberg Coleman Bryson Phillips Grossman PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20016
Phone: 866.252.0878

Email: dlietz@milberg.com

Attorneys for Plaintiffs and
the Proposed Classes

CERTIFICATE OF SERVICE & COMPLIANCE

I hereby certify that on this date I served the foregoing **CONSOLIDATED CLASS ACTION COMPLAINT** via the CM/ECF system, which will automatically provide-email notification and service of such filing to counsel of record for all parties registered with the Court for electronic filing.

This 12th day of June, 2023.

I further certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R. 5.1B.

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson