Exhibit A

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

IN RE: JOHNSON CONTROLS, INC. DATA INCIDENT LITIGATION	Lead Case No.: 25-cv-00955-BHL
This Document Relates To: All Actions	**JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Jennifer C. Gorman, Hal Bauer, Derek Hefley, Carol McKinnon, Frank Waddell, Chris Broadhead, Mohammad Asem Alkhatib, and William John Pacheco, individually and on behalf of all similarly situated persons, allege the following against Johnson Controls, Inc. ("Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents, as to all other matters:

NATURE OF THE ACTION

1. Plaintiffs bring this consolidated class action against Defendant for its failure to properly secure and safeguard Plaintiffs' and other similarly situated Defendant employees' and clients' sensitive information ("Private Information" or "PII[1]").

2. Defendant develops and manufactures building technology such as industrial control systems, security equipment, HVAC systems, and fire safety equipment and claims to offer "the world's largest portfolio of building technology, software and services."[2]

[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] *About Us*, JOHNSON CONTROLS, https://www.johnsoncontrols.com/about-us/our-company (last visited Nov. 29, 2025)

3. Upon information and belief, former and current employees and clients of Defendant are required to entrust Defendant, directly or indirectly, with sensitive, non-public PII, without which Defendant could not perform its regular business activities. Defendant retains this information for many years and even after the employment or client relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. On or about September 24, 2023, Defendant "became aware of a cyber incident that involved the disruption of its information technology infrastructure and resulted in an unauthorized actor having access to and taking data stored on Johnson Controls' network."[3] In response, Defendant commenced an investigation and "determined that an unauthorized actor accessed certain Johnson Controls systems from February 1, 2023 to September 30, 2023 and took information from those systems [the "Data Breach"]."[4]

6. On or about June 30, 2025—more than two years after the Data Breach began—Defendant started issuing public disclosures about the Data Breach.[5]

7. Defendant failed to adequately protect Plaintiffs' and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter

[3] A copy of the letter Defendant sent breach victims and the Office of the Vermont Attorney General about the Data Breach is attached hereto as **Exhibit A**. *See Johnson Controls Data Breach Notice to Consumers*, OFFICE OF THE VERMONT ATTORNEY GENERAL, https://ago.vermont.gov/sites/ago/files/documents/2025-06-30%20Johnson%20Controls%20Data%20Breach%20Notice%20to%20Consumers.pdf (last visited Nov. 29, 2025).
[4] *Id.*
[5] *See, e.g., id.*

failure to protect employees' and clients' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents; and (iv) provide prompt notice of the Data Breach. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

9. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain 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.

10. 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.

11. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

12. Plaintiffs and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

13. Plaintiffs seek remedies including, but not limited to, compensatory damages, nominal damages, and reimbursement of out-of-pocket costs.

14. Plaintiffs also seek injunctive and equitable relief to prevent future injury on behalf of themselves and the putative Class.

PARTIES

15. Plaintiff Jennifer C. Gorman is, and at all relevant times was, an individual citizen and resident of Wisconsin, where she intends to remain.

16. Plaintiff Hal Bauer is, and at all relevant times was, an individual citizen of Texas, where he intends to remain.

17. Plaintiff Derek Hefley is, and at all relevant times was, an individual citizen and resident of Oklahoma, where he intends to remain.

18. Plaintiff Carol McKinnon is, and at all relevant times was, an individual citizen and resident of Missouri, where she intends to remain.

19. Plaintiff Frank Waddell is, and at all relevant times was, an individual citizen and resident of Arizona, where he intends to remain.

20. Plaintiff Chris Broadhead is, and at all relevant times was, an individual citizen and resident of Utah, where he intends to remain.

21. Plaintiff Mohammad Asem Alkhatib is, and at all relevant times was, an individual citizen and resident of California, where he intends to remain. On or about November 19, 2025, pursuant to § 1798.150(b) of the CCPA, Plaintiff Alkhatib separately provided written notice to Defendant identifying the specific provisions of this title he alleges it has violated.

22. Plaintiff William John Pacheco is, and at all relevant times was, an individual citizen and resident of Texas, where he intends to remain.

23. Defendant Johnson Controls, Inc. is a Wisconsin corporation with its principal place of business located at 5757 N Green Bay Ave, Milwaukee, Wisconsin 53209.

JURISDICTION AND VENUE

24. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Class Members are citizens of states that differ from Defendant, including seven of eight Plaintiffs.

25. This Court has personal jurisdiction over Defendant because Defendant is incorporated in, conducts business in, and has sufficient minimum contacts with Wisconsin.

26. Venue is likewise proper as to Defendant in this District under 28 U.S.C. §1391(a)(1) because Defendant's principal place of business is in this District and many of Defendant's acts complained of herein occurred within this District.

FACTUAL ALLEGATIONS

Defendant's Business

27. Defendant offers building technology, software and services for industries such as

healthcare, schools, data centers, airports, stadiums, and hotels.

28. Plaintiffs and Class Members are current and former employees and clients of Defendant.

29. As a condition of receiving employment and/or services, Defendant requires that its employees and clients, including Plaintiffs and Class Members, entrust it with highly sensitive personal information.

30. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiffs and Class Members.

31. Upon information and belief, Defendant made promises and representations to Plaintiffs and Class Members that the PII collected from them as a condition of obtaining employment and/or services from Defendant, would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

32. Indeed, Defendant's Privacy Policy provides in relevant part that:

> At Johnson Controls, we value your privacy and are committed to protecting your personal information in accordance with fair information practices and applicable data privacy laws.
>
> We collect personal information in a variety of ways through normal business activities to enable us to deliver our products and services . . . .
>
> We only collect and process your personal information (including, where legally permissible, special category personal information) for the purposes listed below. Where we are required by law, we will rely on one or more legal bases which may include your prior consent. [6]

[6] *Johnson Controls Privacy Notice*, JOHNSON CONTROLS, https://www.johnsoncontrols.com/trust-center/privacy/global-privacy-notice/johnson-controls-privacy-notice_english (last visited Nov. 29, 2025).

33. Defendant's Employee Privacy Notice states in relevant part:

> Johnson Controls International plc and its affiliated companies (collectively, Johnson Controls) care about your privacy and are committed to processing your Personal Information in accordance with fair information practices and applicable data privacy laws.
> . . . .
>
> 8. Retention
>
> Your Personal Information will be retained as long as necessary to achieve the purpose for which it was collected, usually for the duration of any contractual relationship and for any period thereafter as legally required or permitted by applicable law.
>
> 9. Protection and Security
>
> Johnson Controls takes precautions to protect Personal Information from loss, misuse, and unauthorized access, disclosure, alteration, and destruction. We have taken appropriate technical and organizational measures to protect the information systems on which your Personal Information is stored and we require our suppliers and service providers to protect your Personal Information by contractual and other means.[7]

34. Plaintiffs and Class Members provided their PII to Defendant, directly or indirectly, with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

35. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their

[7] *Employee Privacy*, JOHNSON CONTROLS, https://www.johnsoncontrols.com/legal/employee-privacy (last visited Nov. 29, 2025).

PII.

36. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties and to audit, monitor, and verify the integrity of its systems. Defendant has a legal duty to keep consumer's PII safe and confidential.

37. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

38. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

39. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

The Data Breach

40. On or about June 30, 2025, Defendant filed with the Office of the Vermont Attorney General a notice of public disclosure, informing Plaintiffs and Class Members that:

> WHAT HAPPENED. On September 24, 2023, Johnson Controls became aware of a cyber incident that involved the disruption of its information technology infrastructure and resulted in an unauthorized actor having access to and taking data stored on Johnson Controls' network. We quickly launched an investigation with the support of leading third-party experts and took steps to prevent further access and remove the actor from the network. Based on our investigation, we determined that an unauthorized actor accessed certain Johnson Controls systems from February 1, 2023 to September 30, 2023 and took information from those systems.
>
> WHAT INFORMATION WAS INVOLVED. Given the nature and

> complexity of the data involved, Johnson Controls has been working diligently with a dedicated review team including internal and external experts to conduct a detailed analysis of the data that was taken from Johnson Controls' network. Based on this data analysis, we believe that the unauthorized actor took information about you including your name and [types of personal information].[8]

41. Omitted from the Notice were the details of the root cause of the Data Breach, the vulnerabilities exploited, how many people were impacted by the Data Breach, or what type of PII was stolen by the "unauthorized actor," or what remedial measures were undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

42. This "notice" amounts to no real notice at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without these details, Plaintiffs' and Class Members' ability to mitigate the harm resulting from the Data Breach is severely diminished.

43. And yet, Defendant waited until June 30, 2025, an astonishing 645 days before it began notifying the Class.[9]

44. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

45. And when Defendant did notify Plaintiff and the Class of the Data Breach, Defendant acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiff and the Class:

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

a. "[w] remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring credit reports;"

b. "[y]ou should also be cautious of any unsolicited communications asking for personal information. In addition, if a username and password are listed among your information above, we recommend that you change your login credentials for online accounts"[10]

46. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing its clients' and current and former employees' PII. Thus, Defendant caused widespread injury and monetary damages.

47. Since the breach, Defendant states it has "taken appropriate steps to enhance our security controls."[11]

48. But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented before the Data Breach.

49. Moreover, Defendant has not explained what its "enhanced security controls" actually entails. Thus, upon information and belief, Plaintiffs' and Class Members' PII remains unsecure.

50. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

[10] *Id.*
[11] *Id.*

51. The Notice of Data Breach shows that Defendant cannot—or will not—determine the full scope of the Data Breach, as Defendant has been unable to determine precisely what information was stolen and when.

52. Defendant has done little to remedy its Data Breach. Defendant has offered some victims credit monitoring and identity related services. But such services are wholly insufficient to compensate Plaintiffs and Class members for the injuries that Defendant inflicted upon them.

53. Because of Defendant's Data Breach, the sensitive PII of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

Cybercriminal Group "Dark Angels" is Linked to the Data Breach

54. Based on the technology used in the Data Breach, cybersecurity analysts have linked the Data Breach to the "Dark Angels" ransomware group.[12]

55. Dark Angels operators breach corporate networks and move laterally until they eventually gain administrative access.[13] During this time, they also steal data from compromised servers, which is later used as additional leverage when making ransom demands.[14]

56. Dark Angels also operates a data leak site named "Dunghill Leaks" that is used to extort its victims, threatening to leak data if a ransom is not paid.[15]

---

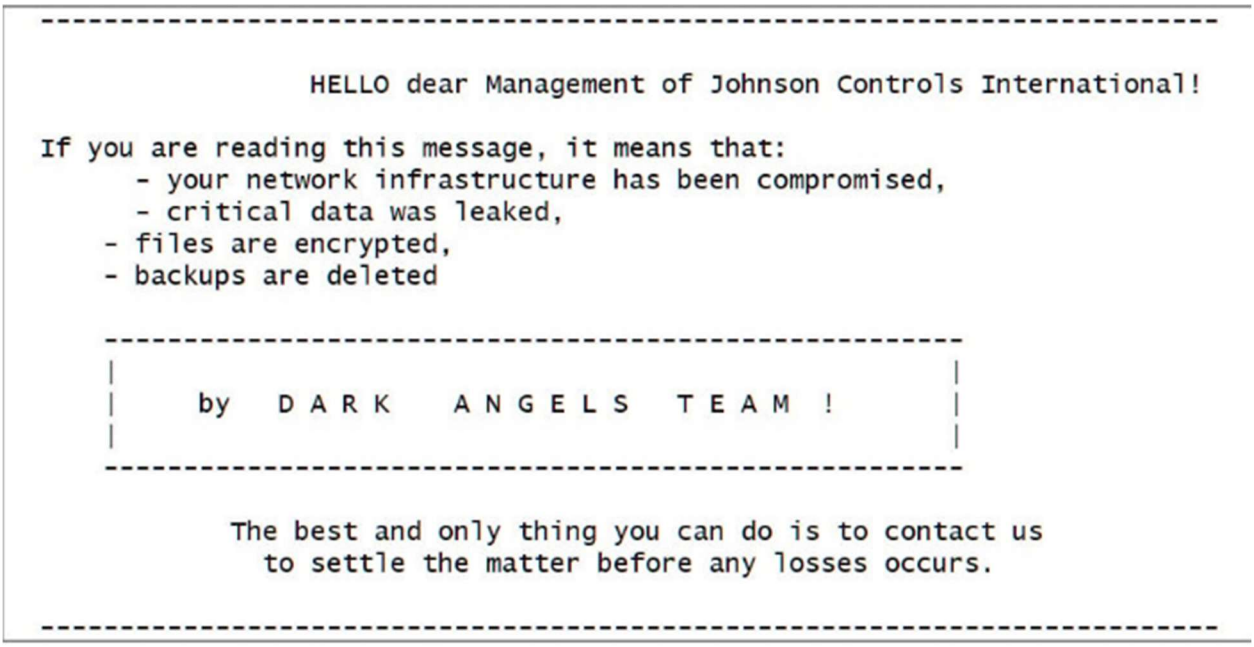
[12] Sergiu Gatlan, *Johnson Controls starts notifying people affected by 2023 breach*, BLEEPING COMPUTER (July 1, 2025), https://www.bleepingcomputer.com/news/security/johnson-controls-starts-notifying-people-affected-by-2023-breach.

[13] Lawrence Abrams, *Dark Angels ransomware receives record-breaking $75 million ransom*, BLEEPING COMPUTER (Julu 30, 2024), https://www.bleepingcomputer.com/news/security/dark-angels-ransomware-receives-record-breaking-75-million-ransom/.

[14] *Id.*

[15] *Id.*

57. On September 27, 2023 Nextron Systems threat researcher Gameel Ali tweeted a sample of a Dark Angels' encryptor containing a ransom note stating it was used against Johnson Controls." [16]



58. Bleeping Computer, an information security and technology news publication, reported that the ransom note linked to a negotiation chat between Defendant and Dark Angels stated that the ransomware gang demanded $51 million for a decryptor and to delete data stolen from Johnson Controls' network.

59. It was further reported that Dark Angels encrypted Defendant's VMware ESXi virtual machines during the attack and claimed to have stolen over 27 TB of documents containing corporate data.

60. To date, Defendant has not made any public statements regarding Dark Angels or whether it made a ransomware payment.

[16] *Id.*

61. On information and belief, even if Defendant paid a ransom demand, this would not ensure the security of Plaintiffs' and the Class's PII. While ransomware groups usually remove stolen data from their data leak sites when a ransom is paid, there is no guarantee that the data will be deleted. That data is valuable and can easily be sold to another threat actor, so there is little incentive to delete it.

62. Defendant confirmed that data was exfiltrated in a ransomware attack it its November 13, 2023 filing with the Securities and Exchange Commission, where it stated the Data Breach "consisted of unauthorized access and deployment of ransomware by a third party" and that it continued to analyze the "data accessed, exfiltrated or otherwise impacted."[17]

63. As the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[18]

64. Thus, on information and belief, Plaintiffs' and the Class's stolen PII has already been published by Dark Angels on the dark web.

Data Breaches Are Preventable

65. Defendant could have prevented this Data Breach by, among other things, properly encrypting PII on its network or otherwise ensuring that such PII was protected while in transit or accessible.

66. Defendant did not use reasonable security procedures and practices appropriate to

[17] Johnson Controls, Inc. (13 Nov. 2023). *Form 8-K 2023*. Retrieved from SEC EDGAR website https://www.sec.gov/Archives/edgar/data/833444/000083344423000038/jci-20231113.htm.
[18] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

67. The unencrypted PII of Class Members will end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

68. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[19]

69. To prevent and detect cyber-attacks and/or ransomware attacks Defendant 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.

[19] *How to Protect Your Networks from RANSOMWARE*, at 3, FBI *et al*., https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Nov. 29, 2025).

- 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.[20]

70. To prevent and detect cyber-attacks or ransomware attacks Defendant 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;

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

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[21]

71. Given that Defendant was storing the PII of its current and former employees and clients, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

72. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of approximately 53,209 current and former employees and

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

clients of Defendant, including that of Plaintiffs and Class Members.

Defendant Acquires, Collects, And Stores Plaintiffs' and the Class's PII

73. As a condition to obtain employment and/or services from Defendant, Plaintiffs and Class Members were required to give their sensitive and confidential PII, directly or indirectly, to Defendant.

74. Defendant retains and stores this information and derives a substantial economic benefit from the PII that they collect. But for the collection of Plaintiffs' and Class Members' PII, Defendant would be unable to offer employment and/or provide services to Plaintiffs and Class Members.

75. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

76. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

77. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiffs and Class Members or by exercising due diligence in selecting its IT vendors and properly auditing those vendors' security practices.

78. Upon information and belief, Defendant made promises to Plaintiffs and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

79. Indeed, Defendant's Privacy Policy provides that:

> We apply appropriate technical, physical and organizational measures that are reasonably designed to protect personal information against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access, and against other unlawful forms of processing.
> . . . .
>
> We will retain your personal information as long as necessary to provide the products you have requested, or to otherwise achieve the purpose for which the personal information was collected and processed. Typically, information is retained for the duration of any contractual relationship, or for as long as the information is required for other legitimate business purposes such as resolving disputes, complying with our legal obligations and enforcing our agreements, or as permitted by applicable law.[22]

80. Defendant's 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.

Defendant Knew or Should Have Known of the Risk Because Companies in Possession of PII Are Particularly Suspectable to Cyber Attacks

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

82. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they keep in their custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access

83. In 2024, there were 3,158 data breaches with 1,350,835,988 victim notices, a 211% increase year over year.[23]

---

[22] *See Johnson Controls Privacy Notice*, note 6, *supra*.
[23] *2024 Data Breach Report* at 6, IDENTITY THEFT RESOURCE CENTER (Jan. 2025),

84. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[24]

85. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

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

87. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant'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.

88. Additionally, as companies became more dependent on computer systems to run their business,[25] e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of

---

https://www.idtheftcenter.org/wp-content/uploads/2025/02/ITRC_2024DataBreachReport.pdf.

[24] Ben Kochman, *FBI, Secret Service Warn Of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection.

[25] Danny Brando *et al*., *Implications of Cyber Risk for Financial Stability*, FEDS NOTES (May

Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[26]

89. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially over one million individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

90. In the Notice, Defendant offers to cover credit monitoring services for a period of 24 months. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity and/or credit monitoring services.

91. Defendant's offer of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive PII was in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

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

93. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs and

12, 2022), https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html.

[26] Dr. Suleyman Ozarslan, *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022*, PICUS LABS (Mar. 24, 2022), https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022.

Class Members are long-lasting and severe. Once PII is stolen fraudulent use of that information and damage to victims may continue for years.

94. As a company in possession of its current and former employees' and clients' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Personally Identifiable Information

95. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[27] 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."[28]

96. 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.[29]

[27] 17 C.F.R. § 248.201 (2013).
[28] *Id.*
[29] *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

97. For example, PII can be sold at a price ranging from $40 to $200.[30] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[31]

98. 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. The information compromised in this Data Breach is impossible to "close" and difficult to change.

99. 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 . . . [is] worth more than 10x on the black market."[32]

100. 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.

101. The fraudulent activity resulting from the Data Breach may not come to light for years. 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.[33]

---

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

[31] *For Sale in the Dark*, VPNOVERVIEW, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Nov. 29, 2025).

[32] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[33] *Report to Congressional Requesters*, GAO, at 29 (June 2007),

Defendant Failed to Comply with FTC Guidelines

102. 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. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. See, e.g., FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

103. In October 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses. The 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. 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 into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

104. 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 the network for suspicious activity, and verify that third-party service providers have implemented reasonable

https://www.gao.gov/assets/gao-07-737.pdf.

security measures.

105. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

106. These FTC enforcement actions include actions against companies like Defendant.

107. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

108. Defendant was at all times fully aware of its obligation to protect the PII of its employees and clients yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Failed to Comply with Industry Standards

109. As noted above, experts studying cybersecurity routinely identify companies like Defendant as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

110. Some industry best practices that should be implemented by companies dealing with sensitive PII, like Defendant, include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware

software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

111. Other best cybersecurity practices that are standard include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

112. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

113. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Defendant Breached its Duty to Safeguard Plaintiffs' and Class Members' PII

114. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately

protected the PII of Class Members

115. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data and failed to audit, monitor, or ensure the integrity of its vendor's data security practices. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect employees' and clients' PII;

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

d. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

e. Failing to sufficiently train its employees and vendors regarding the proper handling of its employees' PII;

f. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

g. Failing to adhere to the industry standards for cybersecurity as discussed above; and

h. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' PII.

116. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted PII.

117. Had Defendant remedied the deficiencies in its information storage and security systems or those of its vendors and affiliates, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class

Members' confidential PII.

Common Injuries & Damages

118. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; I invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

The Data Breach Increases Victims' Risk of Identity Theft

119. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

120. The unencrypted PII of Class Members will end up for sale on the dark web because that is the modus operandi of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

121. 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. 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.

122. 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.

123. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. 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 can be the starting point for these additional targeted attacks on the victim.

124. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[34]

125. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to

[34] "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, 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/.

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.

126. 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 Plaintiffs' 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.

127. 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 driver's license numbers) of Plaintiffs and the other Class Members.

128. Thus, even if certain information (such as a driver's license number) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

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

Loss of Time to Mitigate Risk of Identity Theft and Fraud

130. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

131. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's Notice instructs,[35] "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

132. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as researching and verifying the legitimacy of the Data Breach.

133. These efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), 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.[36]

Diminution Value of PII

134. PII is a valuable property right.[37] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

135. An active and robust legitimate marketplace for PII exists. In 2019, the data

[35] Ex. A.

[36] *See Identity Theft.gov*, FEDERAL TRADE COMMISSION, https://www.identitytheft.gov/Steps (last visited July 7, 2025).

[37] *See, e.g.,* Randall T. Soma, *et al., Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

brokering industry was worth roughly $200 billion.[38]

136. 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.[39,40]

137. As a result of the Data Breach, Plaintiffs' 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 Plaintiffs 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.

138. 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. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

139. 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.

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

141. At all relevant times, Defendant knew, or reasonably should have known, of the

[38] David Lazarus, *Shadowy data brokers make the most of their invisibility cloak*, LA TIMES (Nov. 5, 2029), https://www.latimes.com/business/story/2019-11-05/column-data-brokers.
[39] *See Home Page*, DATA COUP, https://datacoup.com/ (last visited Nov. 29, 2025).
[40] *See Meet World Data Exchange*, WORLD DATA EXCHANGE, https://worlddataexchange.com/about (last visited Nov. 29, 2025).

importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant'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.

142. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to thousands of individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

144. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

145. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that to unemployment benefits were filed for until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

146. Consequently, Plaintiffs and Class Members are at a present and continuous risk

of fraud and identity theft for many years into the future.

147. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Loss of the Benefit of The Bargain

148. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for products and/or services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the product and/or service and necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received products and/or services that were of a lesser value than they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiffs' Experiences and Injuries

Plaintiff Jennifer C. Gorman

149. Plaintiff Gorman is an employee of Defendant.

150. Thus, Defendant obtained and maintained Plaintiff Gorman's PII. As a result, Plaintiff Gorman was injured by Defendant's Data Breach.

151. As a condition of her employment, Plaintiff Gorman provided Defendant with her PII. Defendant used that PII to facilitate its business.

152. Plaintiff Gorman provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and

federal law. Defendant obtained and continues to maintain Plaintiff Gorman's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

153. Plaintiff Gorman reasonably understood that a portion of the funds paid to Defendant (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of PII.

154. Plaintiff Gorman received Defendant's Breach Notice.

155. To the best of her knowledge, Plaintiff Gorman's PII has not been exposed in another data breach, except the Data Breach at issue here.

156. On information and belief, as a result of the Data Breach, Plaintiff Gorman's PII has already been published by cybercriminals on the dark web.

157. On information and belief, as a result of the Data Breach, Defendant compromised at least Plaintiff Gorman's name and Social Security number.

158. Because of the Data Breach, Plaintiff has already suffered from numerous instances of identity theft and fraud. Indeed, since the Data Breach occurred, on or around January 2024, Plaintiff Gorman's Capital One account was hacked, resulting in over $3,000 being withdrawn without her authorization, including the first paycheck Plaintiff Gorman received in January 2024.

159. Further, unauthorized Zelle transactions were also made from Plaintiff Gorman's account, along with multiple microtransactions in and out of the account. As a result of the fraud, Plaintiff Gorman was forced to close all four of her credit cards and spend time reporting these issues to the bank.

160. Additionally, unauthorized cable-TV accounts were opened in Plaintiff Gorman's name in November and December of 2023, and in January of 2024.

161. Moreover, in December of 2024, two loan applications were attempted in Plaintiff Gorman's name through a payday loan provider. Because of the unauthorized applications, Plaintiff Gorman's credit score dropped by 240 points. Plaintiff Gorman was forced to freeze her credit for two years to prevent further fraudulent activity.

162. Plaintiff Gorman has spent several months addressing the impact of the Data Breach — reviewing credit reports and financial account statements, contacting Johnson Controls, enrolling in credit monitoring, communicating with her bank, researching the data breach, and reaching out to the IRS.

163. And in the aftermath of the Data Breach, Plaintiff Gorman has suffered from a spike in scam, spam, and phishing text messages and phone calls.

164. Once an individual's PII is for sale and access on the dark web, as Plaintiff Gorman's is here as a result of the breach, cybercriminals are able to use the stolen and compromised data to gather and steal even more information. On information and belief, the spam, scam, and phishing communications that Plaintiff Gorman is experiencing were made possible as a result of Defendant's Data Breach and the subsequent exposure of Plaintiff's PII to cybercriminals.

165. Plaintiff Gorman fears for her personal financial security and worries about what information was exposed in the Data Breach.

166. Because of Defendant's Data Breach, Plaintiff Gorman has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Gorman's injuries are precisely the type of injuries that the law contemplates and addresses.

167. Plaintiff Gorman suffered actual injury from the exposure and theft of her PII and its threatened or actual publication on the dark web—which violates her rights to privacy.

168. Plaintiff Gorman suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

169. Plaintiff Gorman suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Gorman's PII in the hands of cybercriminals.

170. Because of the Data Breach, Plaintiff Gorman anticipates spending considerable amounts of time and money to try and mitigate her injuries.

171. Today, Plaintiff Gorman has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from additional breaches.

Plaintiff Hal Bauer

172. Plaintiff Hal Bauer was an employee of Defendant from on or around 2015 through on or around 2017.

173. Thus, Defendant obtained and maintained Plaintiff Bauer's PII. As a result, Plaintiff Bauer was injured by Defendant's Data Breach.

174. As a condition of his employment, Plaintiff Bauer provided Defendant with his PII. Defendant used that PII to facilitate its business.

175. Plaintiff Bauer provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and

federal law. Defendant obtained and continues to maintain Plaintiff Bauer's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

176. Plaintiff Bauer reasonably understood that a portion of the funds paid to Defendant (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of PII.

177. Plaintiff Bauer received Defendant's Breach Notice.

178. To the best of his knowledge, Plaintiff Bauer's PII has not been exposed in another data breach, except the Data Breach at issue here.

179. On information and belief, as a result of the Data Breach, Plaintiff Bauer's PII has already been published by cybercriminals on the dark web.

180. On information and belief, as a result of the Data Breach, Defendant compromised at least Plaintiff Bauer's name and Social Security number.

181. Because of the Data Breach, Plaintiff Bauer has already suffered from numerous instances of identity theft and fraud. Indeed, since the Data Breach occurred, four unrecognized charges appeared on Plaintiff Bauer's credit card account with Bank of America in or around 2024. Plaintiff Bauer was forced to replace his credit card three times.

182. Further, from Plaintiff Bauer's Bank of America account, $560.00 was withdrawn and deposited into an unknown and unauthorized Capital One account.

183. Due to the fraud, Plaintiff Bauer has had to spend time contacting his financial institution, reporting the fraud, cancelling his cards, replacing the cards, and reviewing his financial statements. Plaintiff Bauer estimates he has spent over 40 hours addressing the fraud caused by the Data Breach.

184. Plaintiff Bauer has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft.

185. In the aftermath of the Data Breach, Plaintiff Bauer has suffered from a spike in scam, spam, and phishing text messages and phone calls.

186. And in the aftermath of the Data Breach, Plaintiff Bauer received alerts from McAfee and Dash Lane that his PII is circulating on the dark web.

187. Once an individual's PII is for sale and access on the dark web, as Plaintiff Bauer's is here as a result of the breach, cybercriminals are able to use the stolen and compromised data to gather and steal even more information. On information and belief, the spam, scam, and phishing communications that Plaintiff Bauer is experiencing were made possible as a result of Defendant's Data Breach and the subsequent exposure of Plaintiff Bauer's PII to cybercriminals.

188. Plaintiff Bauer fears for his personal financial security and worries about what information was exposed in the Data Breach.

189. Because of Defendant's Data Breach, Plaintiff Bauer has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Bauer's injuries are precisely the type of injuries that the law contemplates and addresses.

190. Plaintiff Bauer suffered actual injury from the exposure and theft of his PII and its threatened or actual publication on the dark web—which violates his rights to privacy.

191. Plaintiff Bauer suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

192. Plaintiff Bauer suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Bauer's PII in the hands of cybercriminals.

193. Because of the Data Breach, Plaintiff Bauer anticipates spending considerable amounts of time and money to try and mitigate his injuries.

194. Today, Plaintiff Bauer has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from additional breaches.

Plaintiff Derek Hefley

195. Plaintiff Derek Hefley was an employee of Defendant from on or around 2006 to on or around 2009.

196. Thus, Defendant obtained and maintained Plaintiff Hefley's PII. As a result, Plaintiff Hefley was injured by Defendant's Data Breach.

197. As a condition of his employment, Plaintiff Hefley provided Defendant with his PII. Defendant used that PII to facilitate its business.

198. Plaintiff Hefley provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Hefley's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

199. Plaintiff Hefley reasonably understood that a portion of the funds paid to Defendant (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of PII.

200. Plaintiff Hefley received Defendant's Breach Notice.

201. To the best of his knowledge, Plaintiff Hefley's PII has not been exposed in another data breach, except the Data Breach at issue here.

202. On information and belief, as a result of the Data Breach, Plaintiff Hefley's PII has already been published by cybercriminals on the dark web.

203. On information and belief, as a result of the Data Breach, Defendant compromised at least Plaintiff Hefley's name and Social Security number.

204. Because of the Data Breach, Plaintiff Hefley has already suffered from identity theft and fraud. Indeed, since the Data Breach occurred, an unauthorized individual gained full access to Plaintiff Hefley's Allegiant Airline Bank of America account on or about September 2024 and initiated a balance transfer of $2,000 dollars. Plaintiff Hefley was forced to spend time reporting the fraud to Bank of America. Plaintiff Hefley estimates he has spent 10 to 20 hours addressing the fraud caused by the Data Breach.

205. Plaintiff Hefley has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft.

206. In the aftermath of the Data Breach, Plaintiff Hefley has suffered from a spike in scam, spam, and phishing text messages and phone calls.

207. Once an individual's PII is for sale and access on the dark web, as Plaintiff Hefley's is here as a result of the breach, cybercriminals are able to use the stolen and compromised data to gather and steal even more information. On information and belief, the spam, scam, and phishing communications that Plaintiff Hefley is experiencing were made possible as a result of Defendant's Data Breach and the subsequent exposure of Plaintiff Hefley's PII to cybercriminals.

208. Plaintiff Hefley fears for his personal financial security and worries about what information was exposed in the Data Breach.

209. Because of Defendant's Data Breach, Plaintiff Hefley has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Hefley's injuries are precisely the type of injuries that the law contemplates and addresses.

210. Plaintiff Hefley suffered actual injury from the exposure and theft of his PII and its threatened or actual publication on the dark web—which violates his rights to privacy.

211. Plaintiff Hefley suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

212. Plaintiff Hefley suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Hefley's PII in the hands of cybercriminals.

213. Because of the Data Breach, Plaintiff Hefley anticipates spending considerable amounts of time and money to try and mitigate his injuries.

214. Today, Plaintiff Hefley has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from additional breaches.

Plaintiff Chris Broadhead

215. Plaintiff Chris Broadhead was an employee of Defendant from on or around 2019 to on or around 2024.

216. Plaintiff Broadhead was a customer of Defendant from on or around 2005 to on or around 2024.

217. Thus, Defendant obtained and maintained Plaintiff Broadhead's PII. As a result, Plaintiff Broadhead was injured by Defendant's Data Breach.

218. As a condition of his employment and of doing business with Defendant, Plaintiff Broadhead provided Defendant with his PII. Defendant used that PII to facilitate its business.

219. Plaintiff Broadhead provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Broadhead's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

220. Plaintiff Broadhead reasonably understood that a portion of the funds paid to Defendant for its services (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of PII.

221. Plaintiff Broadhead received Defendant's Breach Notice.

222. To the best of his knowledge, Plaintiff Broadhead's PII has not been exposed in another data breach, except the Data Breach at issue here.

223. On information and belief, as a result of the Data Breach, Plaintiff Broadhead's PII has already been published by cybercriminals on the dark web.

224. On information and belief, as a result of the Data Breach, Defendant compromised at least Plaintiff Broadhead's name and Social Security number.

225. Plaintiff Broadhead has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft.

226. Plaintiff Broadhead fears for his personal financial security and worries about what information was exposed in the Data Breach.

227. Because of Defendant's Data Breach, Plaintiff Broadhead has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Broadhead's injuries are precisely the type of injuries that the law contemplates and addresses.

228. Plaintiff Broadhead suffered actual injury from the exposure and theft of his PII and its threatened or actual publication on the dark web—which violates his rights to privacy.

229. Plaintiff Broadhead suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

230. Plaintiff Broadhead suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Broadhead's PII in the hands of cybercriminals.

231. Because of the Data Breach, Plaintiff Broadhead anticipates spending considerable amounts of time and money to try and mitigate his injuries.

232. Today, Plaintiff Broadhead has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from additional breaches.

Plaintiff Frank Waddell

233. Plaintiff Frank Waddell was an employee of Defendant from on or around 1996 to on or around 2024.

234. Thus, Defendant obtained and maintained Plaintiff Waddell's PII. As a result, Plaintiff Waddell was injured by Defendant's Data Breach.

235. As a condition of his employment, Plaintiff Waddell provided Defendant with his PII. Defendant used that PII to facilitate its business.

236. Plaintiff Waddell provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Waddell's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

237. Plaintiff Waddell reasonably understood that a portion of the funds paid to Defendant (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of PII.

238. Plaintiff Waddell received Defendant's Breach Notice.

239. To the best of his knowledge, Plaintiff Waddell's PII has not been exposed in another data breach, other than the Data Breach at issue here.

240. On information and belief, as a result of the Data Breach, Plaintiff Waddell's PII has already been published by cybercriminals on the dark web.

241. On information and belief, as a result of the Data Breach, Defendant compromised at least Plaintiff Waddell's name and Social Security number.

242. Because of the Data Breach, Plaintiff Waddell has already suffered from numerous instances of identity theft and fraud. Indeed, since the Data Breach occurred, in the 2024 tax year, an unauthorized individual used Plaintiff Waddell's PII to file a fraudulent tax return in Plaintiff Waddell's name.

243. Further, two unauthorized charges were made using Plaintiff Waddell's credit card.

244. Due to the fraud, Plaintiff Waddell has had to spend time contacting his financial institutions, reporting the fraud, cancelling his card, replacing the card, and reviewing his financial

statements. Plaintiff Waddell estimates he has spent over 80 hours addressing the fraud caused by the Data Breach.

245. Moreover, on May 5, 2025, Plaintiff Waddell received a notification that his PII was circulating on the dark web.

246. Plaintiff Waddell has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft.

247. In the aftermath of the Data Breach, Plaintiff Waddell has suffered from a spike in scam, spam, and phishing text messages and phone calls.

248. Once an individual's PII is for sale and access on the dark web, as Plaintiff Waddell's is here as a result of the breach, cybercriminals are able to use the stolen and compromised data to gather and steal even more information. On information and belief, the spam, scam, and phishing communications that Plaintiff Waddell is experiencing were made possible as a result of Defendant's Data Breach and the subsequent exposure of Plaintiff Waddell's PII to cybercriminals.

249. Plaintiff Waddell fears for his personal financial security and worries about what information was exposed in the Data Breach.

250. Because of Defendant's Data Breach, Plaintiff Waddell has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Waddell's injuries are precisely the type of injuries that the law contemplates and addresses.

251. Plaintiff Waddell suffered actual injury from the exposure and theft of his PII and its threatened or actual publication on the dark web—which violates his rights to privacy.

252. Plaintiff Waddell suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

253. Plaintiff Waddell suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Waddell's PII in the hands of cybercriminals.

254. Because of the Data Breach, Plaintiff Waddell anticipates spending considerable amounts of time and money to try and mitigate his injuries.

255. Today, Plaintiff Waddell has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from additional breaches.

Plaintiff Mohammad Alkhatib

256. Plaintiff Mohammad Alkhatib was an employee of Defendant from on or around 2021 to on or around 2022.

257. Thus, Defendant obtained and maintained Plaintiff Alkhatib's PII. As a result, Plaintiff Alkhatib was injured by Defendant's Data Breach.

258. As a condition of his employment, Plaintiff Alkhatib provided Defendant with his PII. Defendant used that PII to facilitate its business.

259. Plaintiff Alkhatib provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Alkhatib's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

260. Plaintiff Alkhatib reasonably understood that a portion of the funds paid to Defendant (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of PII.

261. Plaintiff Alkhatib received Defendant's Breach Notice.

262. To the best of his knowledge, Plaintiff Alkhatib's PII has not been exposed in another data breach, other than the Data Breach at issue here.

263. On information and belief, as a result of the Data Breach, Plaintiff Alkhatib's PII has already been published by cybercriminals on the dark web.

264. On information and belief, as a result of the Data Breach, Defendant compromised at least Plaintiff Alkhatib's name and Social Security number.

265. Because of the Data Breach, Plaintiff Alkhatib has already suffered from numerous instances of identity theft and fraud. Indeed, since the Data Breach occurred, in approximately June of 2023, Plaintiff Alkhatib experienced approximately 2–3 fraudulent charges on his Wells Fargo debit card totaling several hundred dollars. The charges originated from states such as Wisconsin and Delaware, places Plaintiff Alkhatib has never visited and has no ties to.

266. Due to the fraud, Plaintiff Alkhatib has had to spend time contacting his financial institutions, reporting the fraud, cancelling his card, replacing the card, and reviewing his financial statements. Plaintiff Alkhatib estimates he has spent over 80 hours addressing the fraud caused by the Data Breach.

267. Johnson Controls had access to Plaintiff Alkhatib's debit card number because it was linked to the checking account used to receive payments from Johnson Controls.

268. Further, in approximately June 2023, Plaintiff Alkhatib received a notification from Robinhood that an unauthorized individual changed his Robinhood account password. Plaintiff

Alkhatib simultaneously received another notification from Robinhood stating that an unauthorized individual was attempting to link an unknown bank account to his Robinhood account. Plaintiff Alkhatib was forced to spend time contacting Robinhood upon receiving the notification and report the unauthorized bank account.

269. Plaintiff Alkhatib's Robinhood account was linked to his Outlook email, which he provided to Johnson Controls.

270. Plaintiff Alkhatib has received so many scam, spam, and phishing emails that Outlook disabled his email account.

271. Plaintiff Alkhatib has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft.

272. Plaintiff Alkhatib fears for his personal financial security and worries about what information was exposed in the Data Breach.

273. Because of Defendant's Data Breach, Plaintiff Alkhatib has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Alkhatib's injuries are precisely the type of injuries that the law contemplates and addresses.

274. Plaintiff Alkhatib suffered actual injury from the exposure and theft of his PII and its threatened or actual publication on the dark web—which violates his rights to privacy.

275. Plaintiff Alkhatib suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

276. Plaintiff Alkhatib suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Alkhatib's PII in the hands of cybercriminals.

277. Because of the Data Breach, Plaintiff Alkhatib anticipates spending considerable amounts of time and money to try and mitigate his injuries.

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

Plaintiff Carol McKinnon

279. Plaintiff Carol McKinnon is a former employee of Defendant, having worked for Defendant from on or about 1996 to on or about 2003.

280. Thus, Defendant obtained and maintained Plaintiff McKinnon's PII. As a result, Plaintiff McKinnon was injured by Defendant's Data Breach.

281. As a condition of her employment, Plaintiff McKinnon provided Defendant with her PII. Defendant used that PII to facilitate its business.

282. Plaintiff McKinnon provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff McKinnon's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

283. Plaintiff McKinnon reasonably understood that a portion of the funds paid to Defendant (and/or derived from her employment) would be used to pay for adequate cybersecurity and protection of PII.

284. Plaintiff McKinnon received Defendant's Breach Notice.

285. On information and belief, as a result of the Data Breach, Plaintiff McKinnon's PII has already been published by cybercriminals on the dark web.

286. On information and belief, as a result of the Data Breach, Defendant compromised at least Plaintiff McKinnon's name and Social Security number.

287. Because of the Data Breach, Plaintiff has already suffered from numerous instances of identity theft and fraud. Indeed, since the Data Breach occurred, an unauthorized credit card account was created in Plaintiff McKinnon's name. Plaintiff McKinnon was forced to spend time disputing the fraudulent account with the Credit Bureaus – who sustained Plaintiff McKinnon's dispute. Plaintiff McKinnon estimates she spent over 20 hours addressing the fraud caused by the Data Breach.

288. And in the aftermath of the Data Breach, Plaintiff McKinnon has suffered from a spike in scam, spam, and phishing text messages and phone calls.

289. Once an individual's PII is for sale and access on the dark web, as Plaintiff McKinnon's is here as a result of the breach, cybercriminals are able to use the stolen and compromised data to gather and steal even more information. On information and belief, the spam, scam, and phishing communications that Plaintiff McKinnon is experiencing were made possible as a result of Defendant's Data Breach and the subsequent exposure of Plaintiff McKinnon's PII to cybercriminals.

290. Plaintiff McKinnon fears for her personal financial security and worries about what information was exposed in the Data Breach.

291. Because of Defendant's Data Breach, Plaintiff McKinnon has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go

far beyond allegations of mere worry or inconvenience. Rather, Plaintiff McKinnon's injuries are precisely the type of injuries that the law contemplates and addresses.

292. Plaintiff McKinnon suffered actual injury from the exposure and theft of her PII and its threatened or actual publication on the dark web—which violates her rights to privacy.

293. Plaintiff McKinnon suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

294. Plaintiff McKinnon suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff McKinnon's PII in the hands of cybercriminals.

295. Because of the Data Breach, Plaintiff McKinnon anticipates spending considerable amounts of time and money to try and mitigate her injuries.

296. Today, Plaintiff McKinnon has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from additional breaches.

Plaintiff William John Pacheco

297. Plaintiff William John Pacheco was an employee of Defendant from on or around 2021 to on or around 2024.

298. Thus, Defendant obtained and maintained Plaintiff Pacheco's PII. As a result, Plaintiff Pacheco was injured by Defendant's Data Breach.

299. As a condition of his employment, Plaintiff Pacheco provided Defendant with his PII. Defendant used that PII to facilitate its business.

300. Plaintiff Pacheco provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Pacheco's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

301. Plaintiff Pacheco reasonably understood that a portion of the funds paid to Defendant (and/or derived from his employment) would be used to pay for adequate cybersecurity and protection of PII.

302. Plaintiff Pacheco received Defendant's Breach Notice.

303. To the best of his knowledge, Plaintiff Pacheco's PII has not been exposed in another data breach, except the Data Breach at issue here.

304. On information and belief, as a result of the Data Breach, Plaintiff Pacheco's PII has already been published by cybercriminals on the dark web.

305. On information and belief, as a result of the Data Breach, Defendant compromised at least Plaintiff Pacheco's name and Social Security number.

306. Because of the Data Breach, Plaintiff Pacheco has already suffered from numerous instances of identity theft and fraud. Indeed, since the Data Breach occurred, Plaintiff Pacheco received a letter following the 2023 tax year stating that an unauthorized individual used his Social Security number to file fraudulent tax returns for 3 different employers in California.

307. Further, in 2024, the IRS claimed Plaintiff Pacheco owed $150,000. Plaintiff Pacheco was forced to contact the IRS and file a police report with the local sheriff. Plaintiff Pacheco's dispute with the IRS remains ongoing.

308. Moreover, since 2024, Plaintiff Pacheco has received notifications that unauthorized individuals are attempting to apply for car loans in his name. Because of these fraudulent applications, Plaintiff Pacheco's credit score has dropped 160 points.

309. Plaintiff Pacheco estimates he has spent over 120 hours addressing the fraud caused by the Data Breach.

310. Since the Data Breach, Plaintiff Pacheco has received so much spam, scam and phishing email that he has had to create a new email account. Plaintiff Pacheco also receives more than 5 spam phone calls daily.

311. Once an individual's PII is for sale and access on the dark web, as Plaintiff Pacheco's is here as a result of the breach, cybercriminals are able to use the stolen and compromised data to gather and steal even more information. On information and belief, the spam, scam, and phishing communications that Plaintiff Pacheco is experiencing were made possible as a result of Defendant's Data Breach and the subsequent exposure of Plaintiff Pacheco's PII to cybercriminals.

312. Plaintiff Pacheco has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft.

313. Plaintiff Pacheco fears for his personal financial security and worries about what information was exposed in the Data Breach.

314. Because of Defendant's Data Breach, Plaintiff Pacheco has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Pacheco's injuries are precisely the type of injuries that the law contemplates and addresses.

315. Plaintiff Pacheco suffered actual injury from the exposure and theft of his PII and its threatened or actual publication on the dark web—which violates his rights to privacy.

316. Plaintiff Pacheco suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

317. Plaintiff Pacheco suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Pacheco's PII in the hands of cybercriminals.

318. Because of the Data Breach, Plaintiff Pacheco anticipates spending considerable amounts of time and money to try and mitigate his injuries.

319. Today, Plaintiff Pacheco has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from additional breaches.

CLASS ACTION ALLEGATIONS

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

321. Plaintiffs propose the following nationwide class definition, subject to amendment based on information obtained through discovery:

> All persons in the United States whose Private Information was compromised in the Data Breach (the "Nationwide Class").

322. Plaintiff Alkhatib brings this action on behalf of himself, and all other persons similarly situated pursuant to Fed. R. Civ. P. 23(a) and (b) (the "California Subclass"):

> All California residents whose Private Information was compromised in the Data Breach.

323. Excluded from the Classes are the following individuals and/or entities: Defendant

and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which any Defendant has 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.

324. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

325. Numerosity: The Classes are so numerous that joinder of all members is impracticable. Upon information and belief, thousands of individuals were compromised in the Data Breach.

326. Commonality: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

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

b. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;

c. Whether Defendant had a duty not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

d. Whether Defendant had a duty not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

e. Whether Defendant knew or should have known of the data security vulnerabilities that allowed the Data Breach to occur;

f. Whether Defendant knew or should have known of the risks to Plaintiffs' and Class Members' Private Information in its custody;

g. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;

h. Whether Defendant's data security systems prior to, during, and since the Data Breach complied with industry standards;

i. When Defendant actually learned of the Data Breach;

j. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members of the Data Breach or that their Private Information had been compromised;

k. Whether Defendant violated data breach notification laws by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

l. Whether Defendant conduct violated the FTC Act;

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

n. Whether Defendant adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

o. Whether Defendant breached contracts with its employees made for the benefit of Plaintiffs and Class Members;

p. Whether Defendant was unjustly enriched by failing to provide adequate security for Plaintiffs' and Class Members' Private Information;

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

r. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

s. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm the Data Breach caused.

327. Typicality: Plaintiffs' claims are typical of other Class Members' claims because Plaintiffs and Class Members were subject to the same unlawful conduct as alleged herein and were damaged in the same way. Plaintiffs' Private Information was in Defendant's possession at the time of the Data Breach and was compromised due to the Data Breach. Plaintiffs' damages and injuries are akin to those of other Class Members and Plaintiffs seeks relief consistent with the relief of the Class.

328. Adequacy: Plaintiffs are adequate representatives of the Classes because Plaintiffs are members of the Class and are committed to pursuing this matter against Defendant to obtain relief for the Classes. Plaintiffs have no conflict of interest with the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiffs intend to vigorously prosecute this case and will fairly and adequately protect the interests of all Class Members.

329. Superiority: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to Plaintiffs and Class Members may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiffs and Class Members are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful

conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

330. Manageability: The litigation of the class claims alleged herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate there would be no significant manageability problems with prosecuting this lawsuit as a class action. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

331. Ascertainability: All members of the proposed Class are readily ascertainable. The Class is defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Class. Defendant has access to information regarding the individuals affected by the Data Breach because they are Defendant's current and former employees and customers, and Defendant may have already provided notifications to some or all of those people. Using this information, the members of the Classes can be identified, and their contact information ascertained for purposes of providing notice.

332. Particular Issues: Particular issues are appropriate for certification under Rule 23(c)(4) 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 the following:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

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

d. Whether a contract existed between Defendant and its employees made for the benefit of Plaintiffs and Class Members, and the terms of that contract;

e. Whether Defendant breached the contract;

f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members their Private Information had been compromised;

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

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by misrepresenting its data security processes and vulnerabilities;

i. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members; and

j. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief due to Defendant's wrongful conduct.

333. Policies Generally Applicable to the Classes: Finally, class certification is also appropriate under Rule 23(b)(2) and (c). The Classes are also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to each of the

Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly, and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiffs.

334. Defendant, through uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive and declaratory relief appropriate to the Classes as a whole, including without limitation the following:

a. Ordering Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Ordering that, to comply with Defendant explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to the following:

(i) prohibiting Defendant from engaging in the wrongful and unlawful acts alleged herein;

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

(iii) requiring Defendant to delete and purge the Private Information of Plaintiffs and Class Members unless it 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 Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

(v) requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

(vi) prohibiting Defendant from maintaining Private Information on a cloud-based database until proper safeguards and processes are implemented;

(vii) requiring Defendant to segment data by creating firewalls and access controls so that, if one area of its network is compromised, hackers cannot gain access to other portions of Defendant's systems;

(viii) requiring Defendant to conduct regular database scanning and securing checks;

(ix) requiring Defendant to monitor ingress and egress of all network traffic;

(x) requiring Defendant 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 Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

(xi) requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor its networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated;

(xii) requiring Defendant to meaningfully educate all Class Members about the threats that they because of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

(xiii) Incidental retrospective relief, including but not limited to restitution.

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

335. Plaintiffs restate and reallege the factual allegations set forth above in paragraphs 1-334 as if fully alleged herein.

336. Defendant requires its employees and clients, including Plaintiffs and Class Members, to submit non-public PII in the ordinary course of receiving employment and/or services.

337. Defendant gathered and stored the PII of Plaintiffs and Class Members as part of its business of soliciting employment and services with Defendant, which solicitations and services affect commerce.

338. Plaintiffs and Class Members entrusted Defendant with their PII, directly or indirectly, with the understanding that Defendant would safeguard their information.

339. Defendant 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.

340. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to exercise due diligence in selecting IT vendors and to audit, monitor, and ensure the integrity of its vendor's systems and practices and to give prompt notice to those affected in the case of a data breach.

341. Defendant 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.

342. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

343. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant, Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining employment with Defendant.

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

345. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Class.

346. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII it was no longer required to retain pursuant to regulations.

347. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

348. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity

theft and the fraudulent use of their PII by third parties.

349. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

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

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

c. Failing to audit, monitor, or ensure the integrity of its vendor's data security practices;

d. Allowing unauthorized access to Class Members' PII;

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

f. Failing to remove former employees' PII it was no longer required to retain pursuant to regulations,

g. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

350. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

351. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect, and the type of harm that resulted from the Data Breach was the type of harm these statues were intended to guard against.

352. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

353. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

354. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

355. It was foreseeable that Defendant's 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 Defendant's industry.

356. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if the PII were wrongfully disclosed.

357. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

358. 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.

359. Plaintiffs and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

360. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

361. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

362. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

363. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the PII of Plaintiffs and the Class would not have been compromised.

364. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The PII of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

365. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

366. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

367. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

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

369. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiffs and Class Members in an unsafe and insecure manner.

370. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its 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
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

371. Plaintiffs restate and reallege the factual allegations set forth above in paragraphs 1-370 as if fully alleged herein.

372. Plaintiffs and the Class entrusted their PII to Defendant as a condition of obtaining employment and receiving services from Defendant. In so doing, Plaintiffs and the Class entered

into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen. These implied contracts may be composed, in part, of the written policies posted on Defendant's website, including its Privacy Policy.

373. At the time Defendant acquired the PII of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the PII and not take unjustified risks when storing the PII.

374. Implicit in the agreements between Plaintiffs and Class Members and Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

375. Plaintiffs and the Class would not have entrusted their PII to Defendant had they known that Defendant would make the PII internet-accessible, not encrypt sensitive data elements, and not delete the PII that Defendant no longer had a reasonable need to maintain it.

376. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

377. Defendant breached the implied contracts they made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and the Class once the relationship ended, and by failing to provide timely and

accurate notice to them that personal information was compromised because of the Data Breach.

378. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending 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.

379. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT III
Breach Of Fiduciary Duty
(On Behalf of Plaintiffs and the Nationwide Class)

380. Plaintiffs restate and reallege the factual allegations set forth above in paragraphs 1-379 as if fully alleged herein.

381. In providing their PII, directly or indirectly, to Defendant, Plaintiffs and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiffs and class members to safeguard and keep confidential that PII.

382. Defendant accepted the special confidence Plaintiffs and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiffs' and Class Members' personal information as detailed in its Privacy Policy.

383. In light of the special relationship between Defendant and Plaintiffs and Class members, whereby Defendant became a guardian of Plaintiffs' and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for the benefit of its employees and clients, including Plaintiffs and Class members, for the safeguarding of Plaintiffs and Class member's PII.

384. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of its relationship with Defendant's employees and clients, in particular, to keep secure the PII of its employees and clients.

385. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to protect the integrity of the systems containing Plaintiffs' and Class member's PII.

386. Defendant breached its fiduciary duties to Plaintiffs and class members by otherwise failing to safeguard Plaintiffs' and Class members' PII.

387. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (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) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

388. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
Breach Of Confidence
(On Behalf of Plaintiffs and the Nationwide Class)

389. Plaintiffs restate and reallege the factual allegations set forth above in paragraphs 1-388 as if fully alleged herein.

390. At all times during Plaintiffs and Class members' interactions with Defendant, Defendant was fully aware of the confidential, novel, and sensitive nature of Plaintiffs' and the Class members' PII that Plaintiffs and Class members provided to Defendant.

391. As alleged herein and above, Defendant's relationship with Plaintiffs and Class members was governed by expectations that Plaintiffs and Class members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

392. Plaintiffs and Class members provided their respective PII to Defendant, directly or indirectly, with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized parties.

393. Plaintiffs and Class members also provided their respective PII to Defendant with the explicit understanding that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of information security practices.

394. Defendant voluntarily received in confidence Plaintiffs and Class members' PII with the understanding that the PII would not be disclosed or disseminated to the public or any unauthorized third parties.

395. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, inter alia, failing to follow best information security practices to secure Plaintiffs' and Class members' PII, Plaintiffs' and Class members' PII was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class members' confidence, and without their

express permission.

396. But for Defendant's disclosure of Plaintiffs' and Class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' PII, as well as the resulting damages.

397. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class members' PII. Defendant knew or should have known their security systems were insufficient to protect the PII that is coveted by thieves worldwide. Defendant also failed to observe industry standard information security practices.

398. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT V
Unjust Enrichment / Quasi Contract
(On Behalf of Plaintiffs and the Nationwide Class)

399. Plaintiffs restate and reallege the factual allegations set forth above in paragraphs 1-398 as if fully alleged herein.

400. This count is brought in the alternative to Plaintiffs' breach of implied contract claim.

401. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable PII. In conferring this benefit, Plaintiffs and Class Members understood that part of the benefit Defendant derived from the PII would be applied to data security efforts to safeguard the PII.

402. Defendant appreciated that Plaintiffs and Class Members were conferring a benefit

upon it and accepted that monetary benefit.

403. Acceptance of the benefit under the facts and circumstances described herein make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations 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 Defendant's failure to provide the requisite security.

404. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

405. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

406. If Plaintiffs and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

407. Plaintiffs and Class Members have no adequate remedy at law.

408. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery

from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

409. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

410. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

COUNT VI
Violation of California's Unfair Competition Law (UCL)
Cal. Bus. & Prof. Code § 17200, et seq.
(On Behalf of Plaintiff Alkhatib and the California Subclass)

411. Plaintiff Alkhatib hereby repeats and realleges paragraphs 1 through 410 of this Complaint and incorporates them by reference herein.

412. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

413. Defendant's conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq*. (the "CCPA"), and other state data security

laws.

414. Defendant stored the Private Information of Plaintiff Alkhatib and members of the California Subclass in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff Alkhatib's and the California Subclass's Private Information secure to prevent the loss or misuse of that Private Information.

415. Defendant failed to disclose to Plaintiff Alkhatib and the California Subclass that their Private Information was not secure. However, Plaintiff Alkhatib and the California Subclass were entitled to assume, and did assume, that Defendant had secured their Private Information. At no time were Plaintiff Alkhatib and the California Subclass on notice that their Private Information was not secure, which Defendant had a duty to disclose.

416. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff Alkhatib's and the California Subclass's nonencrypted and nonredacted Private Information.

417. Had Defendant complied with these requirements, Plaintiff Alkhatib and the California Subclass would not have suffered the damages related to the data breach.

418. Defendant's conduct was unlawful, in that it violated the CCPA.

419. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

420. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

421. Defendant's conduct is an unfair business practice under the UCL because it was

immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting Private Information.

422. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

423. Instead, Defendant made the Private Information of Plaintiff Alkhatib and the California Subclass accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff Alkhatib and the California Subclass to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

424. As a result of those unlawful and unfair business practices, Plaintiff Alkhatib and the California Subclass suffered an injury-in-fact and have lost money or property.

425. For one, on information and belief, Plaintiff Alkhatib's and the California Subclass's stolen Private Information has already been published—or will be published imminently—by cybercriminals on the dark web.

426. The injuries to Plaintiff Alkhatib and the California Subclass greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

427. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

428. Therefore, Plaintiff Alkhatib and the California Subclass are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT VII
Violation of the California Consumer Privacy Act
Cal. Civ. Code §§ 1798.100, et. seq. ("CCPA")
(On Behalf of Plaintiff Alkhatib and the California Subclass)

429. Plaintiff Alkhatib hereby repeats and realleges paragraphs 1 through 428 of this Complaint and incorporates them by reference herein.

430. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."

431. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among

other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

432. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

433. Section 1798.150(a)(1) of the CCPA provides:

> "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper."

434. Plaintiff Alkhatib and California Subclass Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

435. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is

collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 100,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

436. The Private Information taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff Alkhatib's and California Subclass Members' unencrypted first and last names and Social Security numbers among other information.

437. Plaintiff Alkhatib's and California Subclass Members' Private Information was subject to unauthorized access and exfiltration, theft, or disclosure because their Private Information was wrongfully taken, accessed, and viewed by an unauthorized third party.

438. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff Alkhatib's and California Subclass Members' Private Information. Defendant failed to implement reasonable security procedures to prevent an attack on their server or network by hackers and to prevent unauthorized access to Plaintiff Alkhatib's and California Subclass Members' Private Information as a result of this attack.

439. On November 19, 2025, Plaintiff Alkhatib provided Defendant with written notice of its violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If Defendant cannot cure

within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

440. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff Alkhatib seeks statutory damages, actual damages, injunctive relief, including public injunctive relief, declaratory relief, and any other relief as deemed appropriate by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and counsel to represent the Class;

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

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

D. 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 Defendant from engaging in the wrongful and unlawful acts described herein;

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

iii. Requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and Class Members unless Defendant 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 Defendant 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 Defendant from maintaining the PII of Plaintiffs and Class Members on a cloud-based database;

vi. Requiring Defendant 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 Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

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

x. Requiring Defendant to conduct regular database scanning and securing checks;

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

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to

appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendant 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; and

xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. 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 Defendant's 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.

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

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and the Class;

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

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: December 3, 2025

Respectfully submitted,

By: */s/ Samuel J. Strauss*

Samuel J. Strauss (WI Bar #1113942)
Raina C. Borrelli
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

Casondra Turner*
Gary M. Klinger
MILBERG, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

Maureen M. Brady*
MCSHANE & BRADY, LLC
4006 Central Street
Kansas City, MO 64111
Telephone: (816) 888-8010
Facsimile: (816) 332-6295
mbrady@mcshanebradylaw.com

Jeff Ostrow*
Ken Grunfeld*
Courtney E. Maccarone*
KOPELOWITZ OSTROW FERGUSON

WEISELBERG GILBERT
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Tel: (954) 525-4100
grunfeld@kolawyers.com
ostrow@kolawyers.com
maccarone@kolawyers.com

Kevin Laukaitis
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Laura Van Note, Esq. (CA S.B. #310160)
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: lvn@colevannote.com

Rachele R. Byrd
WOLF HALDENSTEIN ADLER
FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, California
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com

Jon A. Tostrud (WIED No. 199502)
Anthony M. Carter (WIED No. 39736)
TOSTRUD LAW GROUP, P.C.
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 278-2600
Facsimile: (310) 278-2640
jtostrud@tostrudlaw.com
acarter@tostrudlaw.com

James F. Woods*
Annie E. Causey*

WOODS LONGERGAN PLLC
60 East 42nd Street, Suite 1410
New York, NY 10165
Telephone: (212) 684-2500
jwoods@woodslaw.com
acausey@woodslaw.com

Erik Langeland *
ERIK H. LANGELAND, P.C.
733 Third Avenue, 16th Floor
New York, NY 10017
Telephone: 212-354-6270
elangeland@langelandlaw.com

Blaine Finley*
FINLEY PLLC
1455 Pennsylvania Avenue, NW
Suite 400
Washington, D.C. 20004
Tel.: (281) 723-7904
bfinley@finley-pllc.com

Paul J. Doolittle*
POULIN | WILLEY | ANASTOPOULO
32 Ann Street
Charleston, SC 29403
Telephone: (803) 222-2222
Fax: (843) 494-5536
Email: paul.doolittle@poulinwilley.com
cmad@poulinwilley.com

M. Anderson Berry *
Gregory Haroutunian *
EMERY | REDDY, PC
600 Stewart Street, Suite 1100
Seattle, WA 98101
916.823.6955 (Tel)
206.441.9711 (Fax)
anderson@emeryreddy.com
gregory@emeryreddy.com

David A. Goodwin*
Daniel E. Gustafson*
Michael J. Warkel*
GUSTAFSON GLUEK PLLC
120 South Sixth Street #2600

Minneapolis, MN 55402
Telephone: (612) 333-8844
E-mail: dgoodwin@gustafsongluek.com
dgustafson@gustafsongluek.com
mwarkel@gustafsongluek.com

Amber L. Schubert (CA Bar No. 278696)
SCHUBERT JONCKHEER
& KOLBE LLP
2001 Union St, Ste 200
San Francisco, CA 94123
Tel: (415) 788-4220
Fax: (415) 788-0161
aschubert@sjk.law

Jessica N. Servais (WI #1048014)
Karen Hanson Riebel*
Kate M. Baxter-Kauf*
Emma Ritter Gordon*
Jacob E. Lanthier*
LOCKRIDGE GRINDAL NAUEN, PLLP
100 Washington Ave. S, Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981
jnservais@locklaw.com
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com
erittergordon@locklaw.com
jelanthier@locklaw.com

**Pro Hac Vice forthcoming*

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I, Samuel J. Strauss, hereby certify that I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to counsel of record via the ECF system.

DATED this 3rd day of December, 2025.

STRAUSS BORRELLI PLLC

By: */s/ Samuel J. Strauss*

Samuel J. Strauss
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N. Michigan Ave., Suite 1610
Chicago, IL 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com

— EXHIBIT A —

Return Mail Processing Center
102 W Service Rd # 384
Champlain NY 12919

June 30, 2025

ADFFIN T1 B1 P1 AADC c1 00000001

MT2560S032
000001

[Name]
[Address]

Notice of Data Breach

On behalf of Johnson Controls, we are writing to provide information related to the cyber incident that Johnson Controls became aware of in September 2023, which involved personal information about you. We regret that this incident occurred and take the security of personal information seriously.

WHAT HAPPENED. On September 24, 2023, Johnson Controls became aware of a cyber incident that involved the disruption of its information technology infrastructure and resulted in an unauthorized actor having access to and taking data stored on Johnson Controls' network. We quickly launched an investigation with the support of leading third-party experts and took steps to prevent further access and remove the actor from the network. Based on our investigation, we determined that an unauthorized actor accessed certain Johnson Controls systems from February 1, 2023 to September 30, 2023 and took information from those systems.

WHAT INFORMATION WAS INVOLVED. Given the nature and complexity of the data involved, Johnson Controls has been working diligently with a dedicated review team including internal and external experts to conduct a detailed analysis of the data that was taken from Johnson Controls' network. Based on this data analysis, we believe that the unauthorized actor took information about you including your name and [types of personal information].

WHAT WE ARE DOING. We began investigating the incident as soon as we learned of it. After becoming aware of the incident, we terminated the unauthorized actor's access to the affected systems. In addition, we engaged third-party cybersecurity specialists to further investigate and resolve the incident. We also notified law enforcement and publicly disclosed the incident in filings on September 27, 2023; November 13, 2023; and December 14, 2023. In response to this incident, we have taken appropriate steps to enhance our security controls.

WHAT YOU CAN DO. We do not have reason to believe that the impacted information has been used to cause harm to individuals. Nonetheless, and consistent with certain laws, we are providing you with the following information about steps that you can take to protect against potential misuse of personal information.

As a precaution, we have arranged for you, at your option, to enroll in a complimentary two-year credit monitoring service. We have engaged Equifax to provide you with its Equifax Credit Watch™ Gold, which includes credit monitoring, fraud alerts, identity restoration, identity theft insurance coverage and other features, detailed further on the final page of this letter. **You have until October 31, 2025 to activate the free credit monitoring service by using the following activation code: [Activation Code].** This code is unique for your use and should not be shared. To enroll, go to www.equifax.com/activate

00695-ADFFIN-AUTO-00000001-000001-000-1/2

MT2560S032

You should remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions or the relevant entity with which you hold that account. You should also be cautious of any unsolicited communications asking for personal information. In addition, if a username and password are listed among your information above, we recommend that you change your login credentials for online accounts.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.ftc.gov/idtheft, call the FTC at (877) IDTHEFT (438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from the nationwide credit reporting agencies. If you identify information on your credit report resulting from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax (800) 685-1111 P.O. Box 740241 Atlanta, GA 30374-0241 www.equifax.com	Experian (888) 397-3742 P.O. Box 9701 Allen, TX 75013-9701 www.experian.com	TransUnion (800) 680-7289 Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19022-2000 www.transunion.com

You also have other rights under the Fair Credit Reporting Act ("FCRA". For information about your rights under the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to obtain credit in your name because it tells creditors to follow certain procedures to verify your identity. You may place a fraud alert in your file by calling any of the nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it is required to notify the other two agencies, which then must also place fraud alerts in your file.

You can also contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report. You will need to provide the credit reporting agency with certain information, such as your name, address, date of birth and Social Security number. The credit reporting agency will send you a confirmation containing a unique PIN or password that you will need in order to remove or temporarily lift the freeze. You should keep the PIN or password in a safe place.

FOR MORE INFORMATION. Please know that we regret any inconvenience or concern this incident may cause you. If you have any additional questions or concerns, please go to www.faq.jci.com/english-us or contact us at 1-855-361-0339.

Sincerely,

Johnson Controls

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General
400 6th Street, NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

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

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

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

New York Attorney General
The Capitol
Albany, NY 12224
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, NY 12231
(800) 697-1220
www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

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

North Carolina Department of Justice
Attorney General Jeff Jackson
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.gov

IF YOU ARE A RHODE ISLAND RESIDENT: You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov

****

[Name]
Activation Code: **[Activation Code]**
Enrollment Deadline: **October 31, 2025**

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **[Activation Code]** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*