STATE OF NORTH CAROLINA
MECKLENBURG COUNTY

IN THE GENERAL COURT OF JUSTICE
SUPERIOR COURT DIVISION

LYNNE CURRAN, DEBBIE JEFFERSON, CATHERINE DUNN, DAVE VALENTINE, and DONALD WESCOTT, individually and on behalf of all others similarly situated,

Plaintiff,

v.

HONEYWELL INTERNATIONAL INC.,

Defendant.

Case No.

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Lynne Curran, Debbie Jefferson, Catherine Dunn, Dave Valentine, and Donald Wescott ("Plaintiffs") bring this class action against Defendant Honeywell International Inc. ("Defendant") for its failure to properly secure and safeguard Plaintiffs' and Class Members' personally identifiable information ("PII") stored within Defendant's information network.

INTRODUCTION

1. Defendant is a technology and manufacturing company based in Charlotte, North Carolina.

2. Defendant acquired, collected, and stored Plaintiffs' and Class Members' PII.

3. At all relevant times, Defendant knew or should have known that Plaintiffs and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PII.

4. At no later than the end of May 2023, upon information and belief, unauthorized

third-party cybercriminals gained access to Plaintiffs' and Class Members' PII as hosted with Defendant, with the intent of engaging in the misuse of the PII, including marketing and selling Plaintiffs' and Class Members' PII.

5. The total number of individuals whose data has been exposed due to Defendant's failure to implement appropriate security safeguards is approximately 118,379.

6. Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity and is generally defined to include certain identifiers that do not on their face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

7. The vulnerable and potentially exposed data at issue for Plaintiffs and the Class stored on Defendant's information network includes, without limitation, names and Social Security numbers.

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

9. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiffs and Class Members in the future.

10. Plaintiffs and Class Members have a continuing interest in ensuring that their

information is and remains safe, and they are thus entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

11. The Court has subject matter jurisdiction over this action pursuant to N.C. Const. Art. IV, § 12.

12. This Court has jurisdiction over Honeywell because Honeywell operates in and/or is incorporated in this County.

13. Venue is proper in this Court pursuant to N.C. Gen. Stat. § 1-79 because Defendant is a domestic entity with its principal place of business located in this County, and Honeywell has harmed Class Members residing in this County.

THE PARTIES

Plaintiffs

14. Plaintiff Lynne Curran is an adult individual and, at all relevant times herein, a resident and citizen of Massachusetts. Plaintiff Curran is a victim of the Data Breach.

15. Plaintiff Debbie Jefferson is an adult individual and, at all relevant times herein, a resident and citizen of Illinois. Plaintiff Jefferson is a victim of the Data Breach.

16. Plaintiff Catherine Dunn is an adult individual and, at all relevant times herein, a resident and citizen of Minnesota. Plaintiff Dunn is a victim of the Data Breach.

17. Plaintiff Dave Valentine is an adult individual and, at all relevant times herein, a resident and citizen of Kentucky. Plaintiff Valentine is a victim of the Data Breach.

18. Plaintiff Donald Wescott is an adult individual and, at all relevant times herein, a resident and citizen of Minnesota. Plaintiff Wescott is a victim of the Data Breach.

Defendant Honeywell International Inc.

19. Defendant Honeywell International Inc. is a Delaware corporation whose

principal place of business is 855 S. Mint Street, Charlotte, NC 28202.

CLASS ACTION ALLEGATIONS

20. Plaintiffs bring this action pursuant to the provisions of N.C. Gen. Stat. § 1A-1, R. 23, on behalf of themselves and the following Class:

> All individuals within the United States of America whose PII was exposed to unauthorized third-parties as a result of the data breach experienced by Defendant on May 2023.

21. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which 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 its 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 its immediate family members.

22. Plaintiffs reserve the right to amend the above definitions or to propose subclasses in subsequent pleadings.

23. This action has been brought and may properly be maintained as a class action under N.C. Gen. Stat. § 1A-1, R. 23, because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

24. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Class are so numerous that joinder of all members is impractical, if not impossible. As stated above, over 100,000 people are part of the Class.

25. Commonality: Plaintiffs and the Class Members share a community of interests

in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendant had a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PII;

b. Whether Defendant knew or should have known of the susceptibility of its data security systems to a data breach;

c. Whether Defendant's security procedures and practices to protect its systems were reasonable in light of the measures recommended by data security experts;

d. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

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

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

g. How and when Defendant actually learned of the Data Breach;

h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiffs and Class Members;

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

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by

failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendant's wrongful conduct; and

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

26. Typicality: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

27. Adequacy of Representation: Plaintiffs in this class action are adequate representatives of the Class in that the Plaintiffs have the same interest in the litigation of this case as the Class Members, are committed to the vigorous prosecution of this case, and have retained competent counsel who are experienced in conducting litigation of this nature.

28. Plaintiffs are not subject to any individual defenses unique from those conceivably applicable to other Class Members or the class in its entirety. Plaintiffs anticipate no management difficulties in this litigation.

29. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

30. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

31. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

32. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiffs.

33. Unless a Class-wide injunction is issued, Defendant may continue failing to secure the PII of Class Members properly, and Defendant may continue to act unlawfully as set forth in this Complaint.

34. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under N.C. Gen. Stat. § 1A-1, R. 23.

COMMON FACTUAL ALLEGATIONS

Defendant's Failed Response to the Breach

35. Not until months after it claimed to have discovered the Data Breach did Defendant begin sending the Notice to persons whose PII Defendant confirmed was potentially compromised as a result of the Data Breach.

36. The Notice included, *inter alia*, basic details of the Data Breach, Defendant's recommended next steps, and Defendant's claims that it had learned of the impact of the Data Breach on August 28, 2023, and completed a review thereafter.

37. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' PII with the intent of engaging in the misuse of the PII, including marketing and selling Plaintiffs' and Class Members' PII.

38. Defendant had and continues to have obligations created by law as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiffs' and Class Members' PII confidential and to protect such PII from unauthorized access.

39. Defendant created the reasonable expectation and mutual understanding that, in collecting and storing Plaintiffs' and the Class Members' PII, Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

40. But Defendant breached its duties and obligations in protecting and safeguarding Plaintiffs' and the Class's PII.

41. Plaintiffs and Class Members are, thus, left to speculate as to where their PII ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to

enhance its information security systems and monitoring capabilities to prevent further breaches.

42. Unauthorized individuals can now easily access the PII of Plaintiffs and Class Members.

Defendant Collected/Stored Class Members' PII

43. Defendant acquired, collected, and stored and assured reasonable security over Plaintiffs' and Class Members' PII.

44. As a condition of its relationships with Plaintiffs and Class Members, Defendant required that Plaintiffs and Class Members entrust Defendant with highly sensitive and confidential PII.

45. Defendant, in turn, stored that information in the part of Defendant's system that was ultimately affected by the Data Breach.

46. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was thereafter responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

47. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

48. Plaintiffs and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

49. Defendant could have prevented the Data Breach, which began no later than May 2023, by adequately securing and encrypting and/or more securely encrypting its servers

generally, as well as Plaintiffs' and Class Members' PII.

50. Defendant's negligence in safeguarding Plaintiffs' and Class Members' PII is exacerbated by repeated warnings and alerts directed at protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

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

Defendant Had an Obligation to Protect the Stolen Information

52. Defendant had an obligation to protect Plaintiffs' and Class Members' PII but failed to adequately secure it. As such, Defendant violated its duties because of the Data Breach.

53. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce."[1]

54. 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 Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

55. 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 Plaintiffs and Class

[1] The Federal Trade Commission (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 the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

Members.

56. Defendant owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII was adequately secured and protected.

57. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

58. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would detect a breach in its data security systems immediately and in a timely manner.

59. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

60. Defendant owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

61. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

62. Defendant owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

Plaintiffs' Common Experiences

63. Plaintiffs' information was stored with Defendant as a result of their dealings with Defendant.

64. As required to obtain services from Defendant, Plaintiffs provided Defendant with highly sensitive personal information, who then possessed and controlled it.

65. As a result, Plaintiffs' information was among the data accessed by an unauthorized third-party in the Data Breach.

66. At all times herein relevant, Plaintiffs are and were members of the Class.

67. Plaintiffs each received a letter from Defendant, dated September 14, 2023, stating that their PII was involved in the Data Breach (the "Notice"). *See e.g.*, Exhibit 1.

68. As a result, Plaintiffs were injured in the form of lost time dealing with the consequences of the Data Breach, which included and continues to include: time spent verifying the legitimacy and impact of the Data Breach, time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring their accounts with heightened scrutiny and time spent seeking legal counsel regarding their options for remedying and/or mitigating the effects of the Data Breach.

69. Plaintiffs were also injured by the material risk to future harm they suffer based on Defendant's breach; this risk is imminent and substantial because Plaintiffs' data has been exposed in the breach, the data involved, including Social Security numbers, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's customers, that some of the Class's information that has been exposed has already been misused.

70. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of their PII—a condition of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

71. Plaintiffs, as a result of the Data Breach, have increased anxiety about their loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling their PII.

72. Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII, in combination with their name, being placed in the hands of unauthorized third parties/criminals.

73. Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Value of the Relevant Sensitive Information

74. PII are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

75. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200[2]; Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web[3]; and other sources report that criminals can also purchase access to entire company data breaches from $999 to $4,995.[4]

76. Identity thieves can use PII, such as that of Plaintiffs and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's

[2] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed March 6, 2024).
[3] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed March 6, 2024).
[4] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed March 6, 2024).

picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

77. 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 might 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.[5]

78. Here, Defendant knew of the importance of safeguarding PII and of the foreseeable consequences that would occur if Plaintiffs' and Class Members' PII were stolen, including the significant costs that would be placed on Plaintiffs and Class Members as a result of a breach of this magnitude.

79. As detailed above, Defendant is a large, sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiffs and Class Members. Therefore, its failure to do so is intentional, willful, reckless and/or grossly negligent.

80. Defendant disregarded the rights of Plaintiffs and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training

[5] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed September 19, 2023).

practices in place to adequately safeguard Plaintiffs' and Class Members' PII; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

CLAIMS FOR RELIEF

COUNT ONE
Negligence
(On behalf of the Class)

81. Plaintiffs reallege and reincorporate every allegation set forth in the preceding paragraphs as though fully set forth herein.

82. At all times herein relevant, Defendant owed Plaintiffs and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII of Plaintiffs and Class Members in its computer systems and on its networks.

83. Among these duties, Defendant was expected:

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

b. to protect Plaintiffs' and Class Members' PII using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. to implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

d. to promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

84. Defendant knew that the PII was private and confidential and should be protected as private and confidential and, thus, Defendant owed a duty of care not to subject Plaintiffs and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

85. Defendant knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security.

86. Defendant knew about numerous, well-publicized data breaches.

87. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiffs' and Class Members' PII.

88. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII that Plaintiffs and Class Members had entrusted to it.

89. Defendant breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PII.

90. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiffs and Class Members, Defendant had a duty to adequately protect its data systems and the PII contained therein.

91. Plaintiffs' and Class Members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions.

92. Moreover, only Defendant had the ability to protect its systems, and the PII stored on them from attack. Thus, Defendant had a special relationship with Plaintiffs and Class Members.

93. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiffs' and Class Members' PII and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiffs, and/or the remaining Class Members.

94. Defendant breached its general duty of care to Plaintiffs and Class Members in, but not necessarily limited to, the following ways:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiffs and Class Members;

b. by failing to timely and accurately disclose that Plaintiffs' and Class Members' PII had been improperly acquired or accessed;

c. by failing to adequately protect and safeguard the PII by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII;

d. by failing to provide adequate supervision and oversight of the PII with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiffs and Class Members, misuse the PII and intentionally disclose it to others without consent.

e. by failing to adequately train its employees not to store PII longer than absolutely necessary;

f. by failing to consistently enforce security policies aimed at protecting

Plaintiffs' and the Class Members' PII;

g. by failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h. by failing to encrypt Plaintiffs' and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

95. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

96. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages.

97. The law further imposes an affirmative duty on the Defendant to timely disclose the unauthorized access and theft of the PII to Plaintiffs and Class Members so that they can and/or still can take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

98. Defendant breached its duty to notify Plaintiffs and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiffs and Class Members and then by failing and continuing to fail to provide Plaintiffs and Class Members sufficient information regarding the breach.

99. To date, Defendant has not provided sufficient information to Plaintiffs and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiffs and Class Members.

100. Further, by failing to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking

meaningful, proactive steps to secure their PII.

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

102. Plaintiffs' and Class Members' PII was 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.

103. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

104. The damages Plaintiffs and Class Members have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

105. As a direct and proximate result of Defendant's negligence and negligence *per se*, 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 of 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, tax fraud, 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 embarrassment and identity theft; (vi) lost continuity in relation to their healthcare; (vii) the continued risk to their PII, which may 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 Plaintiffs' and Class Members' PII in its continued possession; and (viii) 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.

106. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members 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.

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

COUNT TWO
Breach of Implied Contract
(On behalf of the Class)

108. Plaintiffs reallege and reincorporate every allegation set forth in the preceding paragraphs as though fully set forth herein.

109. Through its course of conduct, Defendant, Plaintiffs and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' PII.

110. Defendant required Plaintiffs and Class Members to provide and entrust their PII as a condition of obtaining Defendant's services.

111. Defendant solicited and invited Plaintiffs and Class Members to provide their

PII as part of Defendant's regular business practices.

112. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

113. As a condition of being direct consumers of Defendant, Plaintiffs and Class Members provided and entrusted their PII to Defendant.

114. In doing so, Plaintiffs and Class Members entered into implied contracts with Defendant, by which Defendant agreed to safeguard and protect such non-public information, keep such information secure and confidential, and timely and accurately notify Plaintiffs and Class Members if their data had been breached, compromised, or stolen.

115. A meeting of the minds occurred when Plaintiffs and Class Members agreed to, and did, provide their PII to Defendant, in exchange for, amongst other things, the protection of their PII.

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

117. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that their PII was compromised as a result of the Data Breach.

118. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f)

other economic and non-economic harm.

COUNT THREE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Class)

119. Plaintiffs reallege and reincorporate every allegation set forth in the preceding paragraphs as though fully set forth herein.

120. Every contract in this State has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

121. Plaintiffs and Class Members have complied with and performed all conditions of their contracts with Defendant.

122. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of PII and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

123. Defendant acted in bad faith and/or with malicious motive in denying Plaintiffs and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT FOUR
Unjust Enrichment
(On behalf of the Class)

124. Plaintiffs reallege and reincorporate every allegation set forth in the preceding paragraphs as though fully set forth herein.

125. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiffs and Class Members.

126. Defendant, prior to and at the time Plaintiffs and Class Members entrusted their PII to Defendant, caused Plaintiffs and Class Members to reasonably believe that Defendant would keep such PII secure.

127. Defendant was aware, or should have been aware, that reasonable consumers would have wanted their PII kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were sub-standard for that purpose.

128. Defendant was also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiffs' and Class Members' decisions to seek services therefrom.

129. Defendant failed to disclose facts about its substandard information systems, defects, and vulnerabilities before Plaintiffs and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information.

130. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiffs and Class Members the ability to make a rational and informed purchasing and health care decision and took undue advantage of Plaintiffs and Class Members.

131. Defendant was unjustly enriched at the expense of Plaintiffs and Class Members, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiffs and Class Members; however, Plaintiffs and Class Members did not receive the benefit of their bargain because they paid for products and/or services that did not satisfy the purposes for which they bought/sought them.

132. Since Defendant's profits, benefits, and other compensation were obtained

improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

133. Plaintiffs and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiffs and Class Members may seek restitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and each member of the proposed Class, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify the Class and/or any other appropriate subclasses under N.C. Gen. Stat. § 1A-1, R. 23, including the appointment of Plaintiffs' counsel as Class Counsel and appointment of Plaintiffs as Class Representatives;

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

3. That the Court enjoin Defendant, ordering them to cease unlawful activities;

4. 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;

5. 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:

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

b. 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;

c. requiring Defendant to delete 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;

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

e. 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 periodically;

f. prohibiting Defendant from maintaining Plaintiffs' and Class Members' PII on a cloud-based database;

g. requiring Defendant to segment data by 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;

h. requiring Defendant to conduct regular database scanning and securing

checks;

i. 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 PII, as well as protecting the PII of Plaintiffs and Class Members;

j. 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;

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

l. requiring Defendant to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiffs, individually and on behalf of the Class, hereby demand a trial by jury for all issues triable by jury.

Dated: March 20, 2024

Respectfully submitted,

By: */s/ Joel R. Rhine*

RHINE LAW FIRM, P.C.
Joel R. Rhine
jrr@rhinelawfirm.com
North Carolina State Bar No. 16028
Elise Wilson
ehw@rhinelawfirm.com
North Carolina State Bar No. 60366
1612 Military Cutoff, Suite 300
Wilmington, NC 28403
Telephone: (910) 772-9960
Facsimile: (910) 772-9062

FEDERMAN & SHERWOOD
William B. Federman*
10205 N. Pennsylvania Ave.,
Oklahoma City, OK 73120
Telephone: (405) 235-1560
wbf@federmanlaw.com

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

**Pro Hac Vice admission forthcoming*

Attorneys for Plaintiffs and the Class

Honeywell International, Inc.
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 14, 2023

[redacted] J9[redacted]
DONALD M WESCOTT
[redacted]

Re: Notice of Data Breach

Dear Donald M Wescott,

What Happened? We, Honeywell International Inc. ("Honeywell"), 855 Mint St., Charlotte, NC 28202, want to make clear at the outset that keeping personal data safe and secure is very important to us, and we deeply regret that this incident occurred. On August 28, 2023, we determined that your personal information, along with personal information for a small number of other individuals, was among the information that was accessed without authorization.

What Information Was Involved? The information involved may include: your name and social security number.

What We Are Doing. Our security team took prompt steps to address this incident, including contacting law enforcement and blocking the unauthorized access. This notice has not been delayed because of a law enforcement investigation.

In addition, in an abundance of caution, we are offering credit monitoring/identity protection services for a period of 24 months at no cost to you. To take advantage of this offer:

- Ensure that you enroll by: December 31, 2023 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: [redacted]
- Provide your activation code: [redacted]

If you have questions about the product, need assistance with identity protection, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 888-397-0068 by December 31, 2023. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity protection services by Experian.

What You Can Do. It is always a good practice to be vigilant and closely review or monitor your financial accounts, statements, credit reports and other financial information for any evidence of unusual activity, fraudulent charges or signs of identity theft. Please see the attachment for additional information that may be helpful to you.

[redacted]

[redacted] J9[redacted]

For More Information. We take our responsibility to protect your information extremely seriously, and we are very sorry for any inconvenience that this incident may cause you. If you have any questions regarding this incident or the services available to you, assistance is available by calling 888-397-0068 between the hours of 9:00am – 11:00pm EDT Monday through Friday and 11:00am – 8:00pm EDT Saturday and Sunday (excluding major U.S. holidays).

Please note that this notice is personalized for you and that other individuals whose personal data may have been involved will receive their own personalized notices as well.

Sincerely,

Lisa Parlato LeDonne

Lisa Parlato LeDonne
Chief Privacy Officer

Additional Information About Identity Protection Services.

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. *
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 888-397-0068. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL INFORMATION

Please note that you can contact the Federal Trade Commission ("FTC"), your attorney general, and the national consumer reporting agencies for more information on fraud alerts, security freezes and other steps you can take to avoid identity theft:

Equifax, P.O. Box 105788, Atlanta, Georgia 30348, 1-877-478-7625, www.equifax.com

Experian, P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion, P.O. Box 2000, Chester, PA 19016, 1-800-680-7289, www.transunion.com

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, 1-877-FTC-HELP (382-4357), www.ftc.gov/idtheft

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed above.

Additional information about security freezes is included below. Please also note that you can report any suspected incidents of identity theft to law enforcement, your state's attorney general and the FTC. In certain states, you may also obtain any police report filed about this issue. You also have other rights under the Fair Credit Reporting Act ("FCRA"). For further information about your rights under the FCRA, please visit https://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

Additional Information About Security Freezes. You also have a right to place a "security freeze" on your credit report at no charge, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. In addition, a security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

If you wish to place a security freeze on your credit file, you must separately place a security freeze on your credit file at each credit reporting agency. In order to place a security freeze, you may need to provide the following information: (1) Full name (including middle initial as well as Jr., Sr., II, III, etc.); (2) Social Security Number; (3) Date of birth; (4) Addresses for the prior five years; (5) Proof of current address; and (6) A legible copy of a government issued identification card. You can contact each credit reporting agency below for details on what information each company requires and to place a security freeze on your credit file:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
800-349-9960
www.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 160
Woodlyn, PA 19094
888-909-8872
www.transunion.com

[redacted]

[redacted]