Filed: 2/3/2023 3:53 PM
Clerk
Marion County, Indiana

INDIANA COMMERCIAL COURT

STATE OF INDIANA	)	IN THE MARION SUPERIOR COURT 1
	) SS:	
COUNTY OF MARION	)	CAUSE NO._____

RICHARD LILLY, individually and on behalf of all others similarly situated,	)	
	)	CLASS ACTION COMPLAINT
Plaintiff,	)	
v.	)	JURY TRIAL DEMANDED
INDIANAPOLIS HOUSING AGENCY,	)	
Defendant.	)	

CLASS ACTION COMPLAINT

Plaintiff, RICHARD LILLY, individually and on behalf of all others similarly situated ("Plaintiff" or "Lilly") brings this action against Defendant, INDIANAPOLIS HOUSING AGENCY ("Defendant" or "IHA") and alleges as follows:

NATURE OF THE ACTION

1. This is a civil action seeking monetary damages, and injunctive and declaratory relief from Defendant, IHA, a government housing agency, arising from its failure to safeguard the private, highly-sensitive personal information, Personally Identifying Information[1], ("PII") of Plaintiff and approximately 212,910 persons, the proposed Class Members, resulting and the

[1] The Federal Trade Commission defines "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." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendants, not every type of information included in that definition was compromised in the breach.

compromise and unauthorized disclosure of that PII beginning on September 23, 2022, and causing injury and damages to Plaintiff and the proposed Class Members.

2. As explained herein, on information and belief, from on October 4, 2022, IHA discovered that beginning on September 23, 2022 it had experienced a ransomware cyberattack to its information technology computer systems, resulting in authorized access and disclosure of Plaintiff's and the Class Members' PII, including his and/or their names, addresses, dates of birth, and Social Security Numbers, and/or other private, sensitive information (the "Data Breach").[2]

3. Defendant IHA is a governmental public housing agency which provides services to low-income families, seniors, and families with disabilities, better described as providing access for such persons to obtain affordable housing throughout Indianapolis.[3]

4. On or about January 23, 2023, in Defendant's written notice ("Data Breach Notice," Exhibit A) IHA notified Plaintiff Lilly and more than 200,000 customers, the proposed Class Members, that, "[o]n October 4, 2022, IHA was experiencing unusual activity within our IT environment and discovered that the IHA was a victim of a ransomware attack."

5. IHA's Data Breach Notice further represented to Lilly and the proposed Class Members that after the foregoing, IHA, "promptly engaged additional support services, hired security experts and forensics investigators to help us investigate the incident, and ensure the safety of our environment," and, "…also underwent a review of potentially affected data to determine what personal information may have been involved and identify any potentially impacted

[2] *See* IHA Notice of Data Breach to Plaintiff Lilly, January 23, 2023, attached as Exhibit A; and IHA's substantially identical form sample Notice, attached as Exhibit B. *See also*, Maine Attorney General, Data Breach Notifications, available at https://apps.web.maine.gov/online/aeviewer/ME/40/0630de66-2cd4-4da1-a090-84ae591e1a80.shtml (last accessed January 30, 2023).

[3] *See* https://www.indyhousing.org/about/

individuals."[4]

6. Ultimately, IHA's January 23, 2023 Data Breach Notice represented to the persons impacted by the Data Breach that while its "investigation could not confirm [their] personal information was *actually* viewed or misused [;] [t]he information that *may* have been involved included [affected persons'] name, address, date of birth, and other data, including Social Security Numbers."[5]

7. As a result of the Data Breach permitted to occur by IHA, the PII of IHA's current and former customers, was unauthorized disclosed to third-parties and compromised.

8. Upon information and belief, victims of the Data Breach did not start receiving letters notifying them of the Data Breach until January 23, 2023, approximately, four (4) months after the Data Breach occurred and more than three months after it was discovered by IHA. *See* Ex. A.

9. Further, while IHA's Data Breach Notice represented to Plaintiff and the 212,910 other victims of the Data Breach that they had, "no reason to believe that any of [their] information has been or will be misused and the investigation has not revealed any attempts at fraud or identity theft," Defendant offered 12 or 24 months of credit monitoring and identity protection services through IDX at no cost.[6]

10. The foregoing IDX credit monitoring and identity protection is insufficient to compensate Plaintiff or the Class Members for the harm caused to them by the Data Breach.

11. IHA's Data Breach Notice further encouraged the victims of the Data Breach, Plaintiff and the proposed Class Members to "remain vigilant and monitor [their] account

[4] *See* IHA Notice of Data Breach, January 23, 2023, attached as Exhibit A;
[5] *Id.*
[6] *Id.*

statements, financial transactions, and free credit reports for potential fraud and identity theft, and promptly report any concerns."[7]

12. Plaintiff and members of the proposed Class are victims of IHA's failure to honor its privacy policies. Specifically, Plaintiff and members of the proposed Class trusted IHA with their PII. But IHA betrayed that trust. IHA failed to properly use up-to-date security practices to prevent the Data Breach, and when the Data Breach was discovered, Defendant failed to promptly notify victims of the Data Breach of the types of information that was stolen.

13. IHA's tortious conduct and breach of contract, its failure to abide by its privacy policies, caused real and substantial damage to Plaintiff and members of the proposed Class.

14. Further, because this same information remains stored in IHA's systems, Plaintiff and Class members have an interest in ensuring that IHA takes the appropriate measures to protect their PII against future unauthorized disclosures.

15. Plaintiff, Lilly individually and on behalf of all others similarly situated, brings this class action against IHA for failing to adequately secure and safeguard the PII of Plaintiff and the Class, breaching the terms of IHA's implied contracts with its customers, and failing to comply with industry standards regarding the use and transmission of PII.

PARTIES

16. Plaintiff Lilly is a citizen and resident of Missouri, with a principal residence in Jefferson City, Missouri. Plaintiff has received services at IHA, his PII was stored on IHA's computer systems at all times material hereto, and he was a victim in the Data Breach.

17. Defendant IHA is a governmental housing agency with a principal place of business in Marion County, Indianapolis at 1935 N Meridian Street, Indianapolis, Indiana 46202.

[7] *Id.*

JURISDICTION AND VENUE

18. This Court has general personal jurisdiction over IHA because IHA is a citizen of this State.

19. Preferred venue lies in Marion County under Trial Rule 75(A)(4) because Marion County is the county in which IHA maintains its principal office.

FACTUAL ALLEGATIONS

20. Plaintiff Lilly and members of the proposed Class are among the more than 200,000 persons whose PII was unauthorizedly disclosed during the Data Breach.

21. Plaintiff and members of the proposed Class received the Data Breach Notice from IHA, directly informing them for the first time that their PII had been compromised in the Data Breach.

22. According to Defendant, IHA is a "federally-funded government housing agency that provides low-income families, seniors and families with disabilities access to affordable housing in one of our IHA communities or in private market housing subsidized through the Housing Choice Voucher (HCV) Program (Section 8)."[8]

23. IHA provides housing services including "access to safe, decent, affordable housing to Indianapolis families, seniors and persons with disabilities through public housing and the Housing Choice Voucher (HVC) Program (Section 8)," and does so through "federal assistance and mixed-finance funding."[9]

24. Plaintiff, and the proposed Class Members, utilized the services of IHA in accessing subsidized housing.

[8] https://www.indyhousing.org/about/
[9] https://www.indyhousing.org/about/what-we-provide

25. As a condition for receiving services from IHA, Plaintiff and Class members were required by IHA to confide and make available to it, its agents, and its employees, sensitive and confidential PII, including, but not limited to, their names, addresses, dates of birth, and Social Security Numbers, and/or other private, sensitive information.

26. Indeed, IHA allows applicants to make a "pre-application" which requires applicants to provide Defendant, for all persons who will be living in the unit, their names, genders, dates of birth, relationship to the head of household, a current mailing address and telephone number, information on disabilities, gross family annual income (from all sources), all employers (name & address),banking information (name & address), any other sources that could be needed by IHA, Race and ethnicity of the family head, and Social Security Numbers for everyone who will live in the unit.[10]

27. In IHA's online pre-application information website, Defendant promises that, "all information is securely stored and will only be used to add [applicant's] name to our waiting lists."[11]

28. On information and belief, IHA also required an application which required applicants for services to provide their PII, and promised to adequately safeguard the same.

29. IHA acquired, collected, and stored a massive amount of PII of its customers in its computer technology systems.

30. By obtaining, collecting, using, and deriving a benefit from its customers' PII, IHA assumed legal and equitable duties to those individuals and knew or should have known that it was responsible for protecting their PII from unauthorized disclosure.

31. Plaintiff and Class members have taken reasonable steps to maintain the

[10] https://www.indyhousing.org/iha-communities/how-to-apply
[11] Id.

confidentiality of their PII. Plaintiff, as a customer at IHA, relied on IHA to keep his PII confidential and securely maintained, to use this information for business purposes only, and to take reasonable steps to ensure that its vendors would make only authorized disclosures of this information.

32. The Data Breach that is the subject of this civil action is not contemplated or permitted by IHA's pre-application privacy policy.

33. Plaintiff entrusted his PII to IHA solely for the purpose of receiving services in connection with accessing public housing, and with the expectation and implied mutual understanding that IHA would strictly maintain the confidentiality of the information and safeguard it from theft or misuse.

34. Plaintiff would not have entrusted IHA with his highly sensitive PII if he had known that IHA would not adequately protect it from theft, unauthorized use, disclosure, or publication.

A. The Data Breach

35. On information and belief, when Plaintiff presented to IHA for services, its agents represented to Plaintiff, including via its pre-application privacy promises, that it would keep his PII secure.

36. As a prerequisite to receiving services, Plaintiff divulged his personal and highly sensitive PII to IHA, with the implicit understanding that his PII would be kept confidential. This understanding was based on all the facts and circumstances attendant to him receiving services, and the express, specific, written and oral representations made by IHA and its agents.

37. Plaintiff reasonably relied upon IHA's representations to his detriment and would not have provided his sensitive PII to IHA if not for IHA's explicit and implicit promises to adequately safeguard that information.

38. According to IHA as reported to the Maine Attorney General, on or around September 23, 2022, as IHA stated in its Notice of Data Breach, on October 4, 2022, IHA experienced "unusual activity within [its] IT environment and discovered that IHA was the victim of a ransomware attack."

39. After this discovery, IHA "engaged additional support services, hired security experts and forensics investigators to help us investigate the incident, and ensure the safety of our environment. We also underwent a review of potentially affected data to determine what personal information may have been involved and identify any potentially impacted individuals."[12]

40. IHA's Data Breach Notice further stated that:

> We take the confidentiality, privacy, and security of information in our care seriously. We recognize that incidents like this continue to affect large and small organizations throughout the country. We have addressed this matter as thoroughly and expeditiously as possible by conducting a comprehensive investigation into the incident. Since the incident, we have deployed additional cybersecurity measures to enhance the security of our network, and we will be continuously evaluating and evolving our current and future cybersecurity practices to better protect our systems against future attacks.[13]

41. The necessity of IHA utilizing additional cybersecurity measures following the Data Breach evidences the inadequate data security protections Defendants employed prior to the Data Breach, compromising the security of Plaintiff's and the Class Members' PII.

42. While IHA's Data Breach Notice was silent as to when the Data Breach actually occurred, its report to the Maine Attorney General stated the Data Breach occurred on September 23, 2022. Accordingly, the Data Breach began on September 23, 2022 and continued for eleven (11) days undetected, during which time cybercriminals had unauthorized access to the PII of Plaintiff and the Class Members stored on IHA's computer systems.

[12] Ex. A.
[13] Ex. A, B.

43. IHA acknowledges that its patients' highly sensitive PII was compromised by the cybercriminals during the Data Breach. *See* Ex. A.

44. The stolen and published PII of Plaintiff Lilly and the proposed Class Members included their names, addresses, dates of birth, and Social Security Numbers. *See* Exs. A, B.

45. That Data Breach was the direct result of IHA failing to adequately protect the PII of Plaintiff and the Class Members in its care and control, and Defendant's failures to adequately train its employees to prevent such cybersecurity incidents.

46. Despite the highly sensitive nature of the stolen PII and the severe risks associated with its theft, distribution, and publication, upon information and belief, IHA did not notify victims of the Data Breach or about what types of their PII was compromised until on or around January 23, 2023, nearly four (4) months after IHA discovered the Data Breach occurred and three (3) months after IHA discovered the Data Breach.

47. In the Data Breach Notice, IHA recommended that Plaintiff Lilly and members of the Class remain vigilant and monitor their account statements, financial transactions, and free credit reports for potential fraud and identity theft; and, further suggested that affected persons "regularly review bills, notices, and statements, and promptly report any questionable or suspicious activity."[14]

48. In addition, the Data Breach Notice apprised Lilly and the proposed Class Members of their abilities to place fraud alerts with the credit bureaus and to place a security freeze on their credit files.[15]

49. Further still, IHA's Data Breach Notice advised victims that IHA was offering a 1- or 2-year complementary membership with IDX for credit monitoring and identity protection

[14] See Data Breach Notice, Ex. A.
[15] Id.

services, which victims of the Data Breach could sign up for through April 23, 2023. Ex. A at 2.

50. As follows, the IDX credit monitoring and identity protection will not fully compensate Plaintiff or the proposed Class Members for the harm caused by the Data Breach.

51. As a result of this Data Breach, the PII of more than 200,000 individuals whose PII was in the possession of IHA was compromised, including Plaintiff and the proposed Class Members.

52. The Data Breach was preventable and a direct result of IHA's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its customers' PII.

B. The Industry is a Prime Target for Cybercriminals

53. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.[16] The next year, that number increased by nearly 50%.[17]

54. The PII stolen in the Data Breach, including Lilly's Social Security Number, is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach—most notably name, date of birth, and Social Security number—is difficult, if not impossible, to change.

55. This kind of data, as one would expect, demands a much higher price on the dark

[16] *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER ("ITRC") (Jan. 19, 2017), https://bit.ly/30Gew91.
[17] *2017 Annual Data Breach Year-End Review*, ITRC (Jan. 25, 2018), https://bit.ly/3nrzgdH.

web. 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."[18] Likewise, the FBI has warned healthcare organizations that PII data is worth 10 times as much as personal credit card data on the black market.[19]

56. PII data for sale is so valuable because PII is so broad, and it can therefore be used for a wide variety of criminal activity such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining patient numbers with false provider numbers to file fake claims with insurers.

57. The value of Plaintiff's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

58. Plaintiff Lilly has confirmed via Discover that his PII is on the dark web as of Fall of 2022.

C. IHA failed to sufficiently protect the PII that patients had entrusted to it

i. IHA failed to adhere to FTC guidelines

59. According to the Federal Trade Commission ("FTC"), the need for data security

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), https://bit.ly/3DyuUHs.

[19] Stolen PHI health credentials can sell for up to 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber-crime protection company who obtained his data by monitoring underground exchanges where cyber-criminals sell the information. *See* Humer, Caroline & Finkle, Jim, *Your medical record is worth more to hackers than your credit card*, REUTERS (Sep. 24, 2014), https://reut.rs/3qNZZ6o. Dark web monitoring is a commercially available service which, at a minimum, IHA can and should perform (or hire a qualified third-party expert to perform).

should be factored into all business decision-making.[20] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as IHA, should employ to protect against the unlawful exposure of PII.

60. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[21] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

61. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

62. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[22]

63. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

[20] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Sep. 2, 2015), https://bit.ly/3nxT3sc.
[21] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Sep. 28, 2016), https://bit.ly/3oENwiN.
[22] *See Start with Security*, *supra* note 20.

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

64. IHA's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

65. Despite the abundance and availability of information regarding cybersecurity best practices for the industry, IHA failed to adopt sufficient data security processes, including but not limited to those standards set forth in the FTCA.

66. IHA's failure to implement these rudimentary measures made it an easy target for the ransomware Data Breach that came to pass.

D. Plaintiff and the Class Members were significantly harmed by the Data Breach

67. As a direct result of the Data Breach which IHA failed to prevent, on information and belief, Plaintiff's PII entrusted to IHA has been compromised and disclosed to unauthorized parties.

68. As discussed above, PII is among the most sensitive, and personally damaging information. A report focusing on breaches in the healthcare industry found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000.00" per person, and that the victims were further routinely forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[23]

[23] Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://cnet.co/3Dzh5IC.

69. As a result of the Data Breach, Plaintiff now faces, and will continue to face, a heightened risk of identity theft and fraud for the rest of his life.

70. IHA knew or should have known the importance of safeguarding customer PII entrusted to it and of the foreseeable consequences of a breach. Despite this knowledge, however, IHA failed to take adequate cyber-security measures to prevent the ransomware attack from happening.

71. As stated prior, IHA's complimentary IDX credit monitoring and identity theft protection will not fully compensate Plaintiff or the proposed Class Members for the harm caused by the Data Breach.

72. Even if IHA did reimburse Plaintiff and members of the Class for the harms they have suffered, it is incorrect to assume that reimbursing a victim of the Data Breach for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[24]

73. As a result of IHA's failure to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered and will continue to suffer significant damages. They have suffered or are at increased risk of suffering:

a. Fraudulent charges as a result of their PII being publicly available on the Dark Web for sale and other fraudulent misuse;

[24] *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUSTICE 10, 11 (Jan. 27, 2014), https://bit.ly/3x3wJJK.

b. The loss of the opportunity to control how their PII is used;

c. The diminution in value of their PII;

d. The compromise, publication and/or theft of their PII;

e. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud, including the purchase of identity theft protection insurance and detection services;

f. Lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from 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 and fraud;

g. Delay in receipt of tax refund monies;

h. Unauthorized use of stolen PII;

i. The continued risk to their PII, which remains in the possession of IHA and is subject to further breaches so long as they fail to undertake appropriate measures to protect the PII in their possession; and

j. Current and future costs related to the time, effort, and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

74. On information and belief, Plaintiff has already incurred harms as a result of the Data Breach, including mental and emotional stress and anxiety.

75. In addition, Plaintiff has incurred damages relating to the reasonable mitigation efforts that he has employed; Plaintiff has also expended time and effort in order to mitigate the

harm he has suffered on account of the Data Breach.

76. Plaintiff timely and appropriately sent a Tort Claim Notice of this incident pursuant to Indiana Statutes to Defendant IHA on January 31, 2023.

CLASS ACTION ALLEGATIONS

77. Plaintiff brings this action on behalf of himself, and as a class action on behalf of the following proposed class ("the Class"):

> All persons whose personal information was compromised in IHA's Data Breach announced to affected persons on or about January 23, 2023.

78. Excluded from the Class are the officers, directors, and legal representatives of IHA and the judges and court personnel in this case and any members of their immediate families.

79. This action is properly maintainable as a class action under Indiana Rules of Trial Procedure 23(A) and (B)(3).

80. Numerosity. IHA reports that the Data Breach compromised the PII of more than 200,000 individuals. Therefore, the members of the Class are so numerous that joinder of all members is impractical.

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

a. Whether an express contract existed among the Plaintiff and the proposed Class Members and IHA;

b. Whether an implied contract existed among the Plaintiff and the proposed Class Members and IHA;

c. Whether IHA breached their contract(s) with Plaintiff and the proposed Class Members;

d. Whether and to what extent IHA had a duty to protect the PII of Plaintiff and the Class;

e. Whether IHA failed to adopt the practices and procedures necessary to adequately safeguard the information compromised in the Data Breach;

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

g. Whether Class Members are entitled to actual damages, statutory damages, and/or punitive damages as a result of IHA's wrongful conduct;

h. Whether Plaintiff and the Class are entitled to restitution as a result of IHA's wrongful conduct; and

i. Whether Plaintiff and the Class are entitled to injunctive and/or declaratory relief.

82. Typicality. Plaintiff's claims are typical of those of other Class members because Plaintiff's PII, like that of every other Class member, was compromised by the Data Breach permitted to occur by IHA. Further, Plaintiff, like all Class members, was injured by IHA's uniform conduct. Plaintiff is advancing the same claims and legal theories on behalf of herself and all other Class members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of other Class members arise from the same operative facts and are based on the same legal theories.

83. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Class in that he has no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiff suffered are typical of other Class members, and Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class. Plaintiff has retained counsel experienced in

complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

84. Superiority of Class Action. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class's common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based on an identical set of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

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

86. Adequate notice can be given to Class members directly using information maintained in IHA's records.

87. Predominance. Pursuant to Rule 23(B)(3), the issues in this action are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include but are not limited to the questions identified above.

88. It does not appear that other persons who fall within the Class definition set forth above are pursuing similar litigation.

89. This proposed class action does not present any unique management difficulties.

FIRST CAUSE OF ACTION
Breach of Express Contract
(On Behalf of Plaintiff and the Class)

90. Plaintiff restates and re-alleges all preceding paragraphs as if fully set forth herein.

91. Defendant offered to provide public housing assistance services to Plaintiff and Class Members.

92. Plaintiff and Class Members accepted Defendant's offer to provide these services by applying for and receiving the same.

93. IHA required Plaintiff and Class Members to provide their PII including customers' names, addresses, dates of birth, and Social Security Numbers, and/or other private, sensitive information in order to receive Defendant's housing assistance.

94. The Parties' agreement was supported by adequate consideration because Plaintiff and Class Members entrusted their PII to IHA, and received housing assistance from IHA, while under no legal obligation to do so.

95. In its policies, including its pre-application, which was incorporated into the Parties' agreement by reference, IHA expressly promised Plaintiff and the Class Members that Defendant would only disclose PII under certain circumstances, none of which relate to the Data Breach.

96. Included in the agreement between Defendant and its members, including Plaintiff and Class members, was Defendant's obligation to use such PII for business purposes only, to take reasonable steps to secure and safeguard that PII, and not make disclosures of the PII to unauthorized third parties.

97. Plaintiff and the Class Members would not have entrusted their PII to Defendant in the absence of such agreement with Defendant.

98. Defendant materially breached the express and/or implied, unilateral and/or bilateral contract(s) it had entered with Plaintiff and Class Members by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and Class members by:

a. Failing to properly safeguard and protect Plaintiff's and Class Members' PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement;

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendant created, received, maintained, and transmitted.

54. The damages sustained by Plaintiff and Class Members as described above were the direct and proximate result of Defendant's material breaches of its agreements.

55. Plaintiff and Class Members have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

56. Good faith is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

57. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

58. Defendant failed to promptly advise Plaintiff and Class Members of the Data Breach.

59. In these and other ways, Defendant violated its duty of good faith and fair dealing.

60. Plaintiff and Class Members have sustained damages as a result of Defendant's breaches of its agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

99. Plaintiff restates and re-alleges all preceding paragraphs as if fully set forth herein, in the alternate to the First Cause of Action for Breach of Express Contract.

100. Plaintiff and Class members were required to provide their PII—including names, addresses, dates of birth, and Social Security Numbers, and/or other private, sensitive information in order to participate in Defendant's housing assistance —to IHA as a condition of receiving housing assistance services.

101. Implicit in the agreement between IHA and its patients was the obligation that both parties would maintain information, PII, confidentially and securely.

102. IHA had an implied duty of good faith to ensure that the PII of Plaintiff and Class members in its possession was only used to provide public housing assistance services to Plaintiff and the Class Members.

103. IHA had an implied duty to reasonably safeguard and protect the PII of Plaintiff and Class members from unauthorized disclosure or uses.

104. Additionally, IHA implicitly promised to retain this PII only under conditions that kept such information secure and confidential.

105. Plaintiff and Class members fully performed their obligations under the implied contract with IHA. IHA did not. Plaintiff and Class members would not have provided their confidential PII to IHA in the absence of their implied contracts with IHA and would have instead retained the opportunity to control their PII for uses other receiving housing assistance from IHA.

106. IHA breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff and Class members' PII, which was compromised as a result of the Data Breach.

107. IHA's acts and omissions have materially affected the intended purpose of the implied contacts requiring Plaintiff and Class members to provide their PII in exchange for public housing assistance services.

108. As a direct and proximate result of IHA's breach of its implied contacts with Plaintiff and Class members, Plaintiff and Class members have suffered and will suffer injury, and damages, as set forth in the preceding paragraphs, including but not limited to: (i) fraudulent misuse of the PII on the Dark Web; (ii) the loss of the opportunity to control 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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in IHA's possession and is subject to further unauthorized disclosures so long as IHA fails to undertake appropriate and adequate measures to protect the PII of current and former customers that is 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 Plaintiff and Class members.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

109. Plaintiff restates and re-alleges all preceding paragraphs as if fully set forth herein.

110. This claim is pleaded in the alternative to the breach of express and implied contractual duty claims.

111. Plaintiff and members of the Class conferred a benefit upon Defendant in the form of providing their PII to IHA.

112. Defendant appreciated or had knowledge of the benefits conferred upon itself by the receipt of Plaintiff and members of the Class's PII, as this was used to facilitate them receiving public housing assistance services.

113. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff and the proposed Class's PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII to Defendant had they known Defendant would not adequately protect their PII.

114. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by it because of its misconduct and Data Breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, RICHARD LILLY, on behalf of himself and all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representative and his counsel as Class counsel;

B. A mandatory injunction directing IHA to adequately safeguard the PII of Plaintiff and the Class hereinafter by implementing improved security procedures and measures;

C. A mandatory injunction requiring that IHA provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of PII to unauthorized persons;

D. An award of damages, in an amount to be determined;

E. An award of attorneys' fees and costs;

F. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law; and

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: February 3, 2023

Respectfully submitted,

s/ Lynn A. Toops

Lynn A. Toops (No. 26386-49)
Amina A. Thomas (No. 34451-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
(317) 636-6481
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

J. Gerard Stranch IV*
Andrew E. Mize*
BRANSTETTER STRANCH & JENNINGS, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 27203

(615) 254-8801
gerards@bsjfirm.com
andrewm@bsjfirm.com

Counsel for the Plaintiff, Richard Lilly, and the Proposed Class

*Motion for *Pro Hac Vice* forthcoming