IN THE COMMON PLEAS COURT OF FRANKLIN COUNTY, OHIO

JOHN DOE #1, JOHN DOE #2 AND JANE DOE **c/o Counsel** **305 West Nationwide Boulevard** **Columbus, Ohio 43215,** ***On behalf of themselves and all others similarly situated,*** **Plaintiffs,** **v.** **CITY OF COLUMBUS** **c/o Columbus City Attorney** **77 North Front Street** **Columbus, Ohio 43215,** **Defendant.**	:	**Case No. 24CV006195** **Judge Carl Aveni** **DEMAND FOR JURY TRIAL**

FIRST AMENDED CLASS ACTION COMPLAINT

John Doe #1, John Doe #2 and Jane Doe ("Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Class Action Complaint against Defendant the City of Columbus ("the City" or "Defendant"). Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data maintained by Defendant regarding city employees and many members of the public at large.

2. The City maintains, via its consolidated Information Technology (IT) infrastructure, the electronic records for all City operations.

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") and other sensitive information about both its current and former City

employees and citizens who interact with the City in various capacities. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. It is unknown precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to the now-compromised PII.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to maintain reasonable security safeguards or protocols to protect the Class's PII and failed to adequately train its employees on cybersecurity. In short, Defendant's failures placed the Class's PII in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiffs are Data Breach victims. They bring this class action on behalf of themselves, and all everyone harmed by Defendant's misconduct.

7. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this Data Breach, Class Members' private information was exactly that—private. Not anymore. Now, their private information is forever exposed.

PARTIES

8. Plaintiff John Doe #1 is a natural person and citizen of Ohio. He resides in Columbus, Ohio where he intends to remain. He is a Columbus Police Officer, and at present serves as a Patrol Officer.

9. Plaintiff John Doe #2 is a natural person and citizen of Ohio. He resides in Columbus, Ohio where he intends to remain. He is a Columbus Police Officer, and at present serves in an undercover role.

10. Plaintiff Jane Doe is a natural person and citizen of Ohio. She resides in Columbus, Ohio where she intends to remain.

11. Defendant, the City of Columbus, is a municipal corporation pursuant to Ohio Revised Code § 703.1(A). The Defendant is subject to legal process by and through the office of the Columbus City Attorney, 77 North Front Street, Columbus, Ohio 43215.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction under O.R.C. § 2305.01 because this is a civil case and the amount-in-controversy exceeds $15,000.

13. This Court has personal jurisdiction over Defendant because it is a municipal corporation located in this County.

14. Venue is proper in this Court because Defendant is a municipal corporation located in this County, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this County.

15. The activities of Defendant at issue in this litigation—the operation of a city-wide IT infrastructure--are Proprietary Activities as defined by Ohio Revised Code § 2744.01(G)(1), as it is not a governmental activity listed in § 2744.01(C)(1)(a), § 2744.01(C)(1)(b), or § 2744.01(C)(2), and it is a function that "promotes or preserves the public peace, health, safety, or welfare and that involves activities that are customarily engaged in by nongovernmental persons."

16. As such, pursuant to Ohio Revised Code § 2744.02(B)(2), Defendant is "liable for injury, death, or loss to person or property caused by the negligent performance of acts by their employees," as set forth herein.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiffs and the Class

17. Defendant is a municipal corporation located in Franklin County, Ohio. As of the 2020 Census, the City of Columbus had a population of 905,748 people. According to its website, the City employs over 10,000 people.[1]

18. As a municipal corporation, the City maintains a host of city services, including but not limited to first responders such as the Columbus Police Department ("CPD") and the Columbus Fire Department. The City is also responsible for the Franklin County Municipal Court.

19. In connection with providing these services, Defendant has a Department of Technology ("DoT"). According to its website, "[t]he Department of Technology's (DOT) primary mission is supporting and partnering with public facing agencies across the City in using technology to serve the residents and businesses of Columbus and Central Ohio."[2]

20. As part of its duties, Defendant's DoT operates by "planning, designing, developing, procuring, and delivering information technology, telecommunications, and media services in partnership with City departments, City Council, boards and commissions, and other government entities."[3]

---

[1] https://www.columbus.gov/Government/Departments/Technology/Work-with-Us#:~:text=The%20City%20of%20Columbus%20employs,approximately%20650%2B%20different%20job%20titles (last accessed August 6, 2024).

[2] https://www.columbus.gov/Government/Departments/Technology/About-DoT (last accessed August 6, 2024).

[3] *Id*.

21. In the context of maintaining this IT infrastructure, Defendant receives and maintains the PII of thousands of its current and former employees.

22. In addition, Defendant maintains records of non-employee citizens interacting with City government and City services. These records are extensive and include many of the citizens of the City of Columbus and the surrounding area.

23. Among the records in Defendant's IT infrastructure, Defendant maintains records of every person who visits City Hall and other City government buildings, including a complete record of the driver's license information of those visitors (who are required to present a driver's license to enter City Hall).

24. Moreover, Defendant's IT infrastructure includes the full records of the Franklin County Municipal Court maintained by the Clerk and the City Attorney's Office. This includes the contact information for all individuals who have been charged with misdemeanor and citation level offenses (including traffic tickets) in the City of Columbus, as well as contact information for victims of crimes adjudicated by Municipal Court.

25. On information and belief, Defendant maintained a single, unified IT system for all City services and entities.

26. In collecting and maintaining the PII, Defendant agreed it would safeguard the data in accordance with its internal policies, and state and federal law.

27. Under the law, institutions like Defendant have duties to protect the PII in its possession and to promptly notify affected individuals about data breaches.

Defendant's Data Breach

28. On July 19, 2024, the City of Columbus experienced an extensive computer outage affecting many if not all City functions.

29. At 10:31 AM on the 19th, CPD personnel, including Plaintiffs John Doe #1 and John Doe #2, received an alert via email informing them about "an outage that is affecting internet connections." [4]

30. On July 20, 2024, CPD personnel were informed that the outage was persistent, affecting numerous internal systems.[5] These outages were expected to continue into the next week.

31. On July 23, 2024, CPD personnel were informed that the network outage was a result of a "cybersecurity incident," presumably beginning on or about July 19, 2024.[6] At the same time, further guidance was provided to CPD officers and personnel regarding maintaining additional, effective data security practices.[7] Such practices, laudable as they might be, did not and could not mitigate the effects of the breach that had already occurred.

32. On July 29, 2024, Defendant released a press release, published on its website, entitled "Columbus Thwarted Ransomware Encryption of its IT Infrastructure."[8] The release stated that "a foreign cyber threat actor attempted to disrupt the city's IT infrastructure, in a possible effort to deploy ransomware and solicit a ransom payment from the city." It also represented that, "[f]ortunately, the city's Department of Technology quickly identified the threat and took action to significantly limit potential exposure, which included severing internet connectivity."

33. Unfortunately, Defendant did not in fact "thwart" the cyberattack. On or about July 29, 2024, CPD officers began receiving credit alerts relating to suspicious activity in connection with their personal financial accounts and/or reported funds missing from personal bank accounts.

---

4 Exhibit 1.

5 Exhibit 2.

6 Exhibit 3.

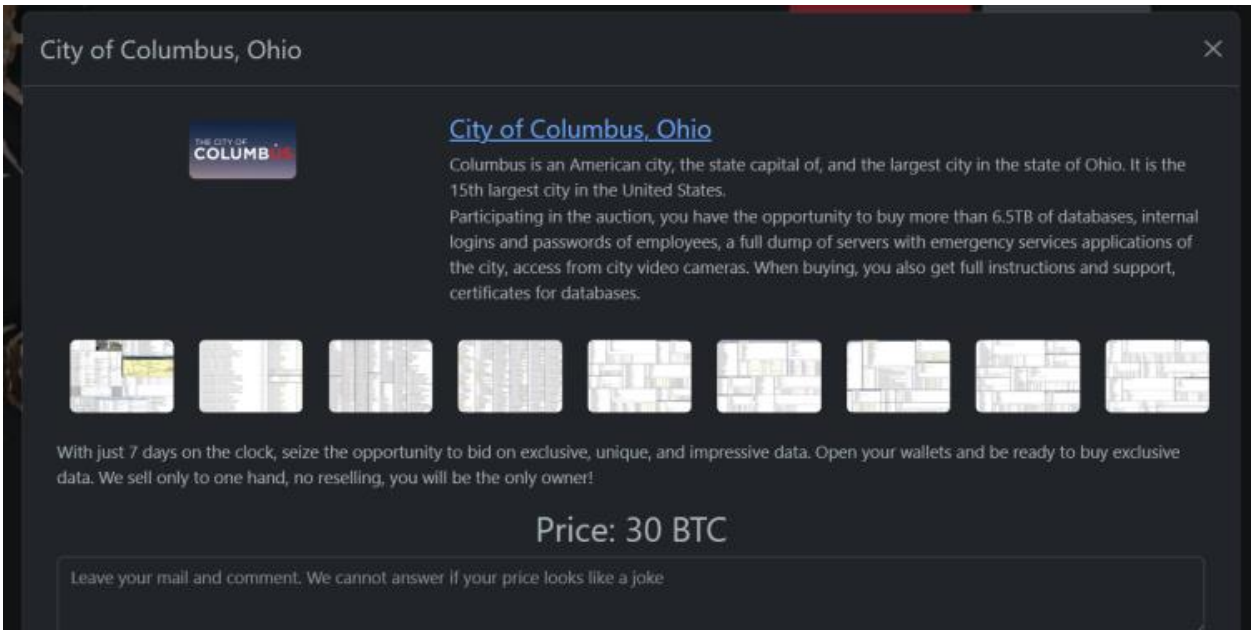
7 Exhibit 4.

8 https://www.columbus.gov/News-articles/City-of-Columbus-Thwarted-Ransomware-Encryption-of-its-IT-Infrastructure (last accessed August 6, 2024).

34. On July 31, 2024, cybercriminals posted on the Internet that they were in possession of most if not all of the data contained in Defendant's systems, including the PII of Class Members. This post represented that the data would be made available for sale on the "Dark Web" if a ransom was not paid.

35. On August 1, 2024, CPD personnel were informed that "we believe some of our data has been accessed."[9] On the same day, CPD personnel were informed that they, alongside all Defendant's employees, Franklin County Municipal Court judges, and Franklin County Municipal Court Clerk employees would receive two years of free credit monitoring services.

36. Moreover, on information and belief, Class Members' data has been made available to nefarious actors and cybercriminals on the "Dark Web." As of August 5, 2024, a posting is accessible on the "Tor" service encouraging cybercriminals to participate in an auction to receive access to the Class Members' data.



9 Exhibit 5.

37. The post represents that the data provided for auction represents 6.5 Terabytes of data, including "internal login and passwords of employees, a full dump of servers with emergency services applications of the city, [and] access from city video cameras." The post also shows what appears to be folder architectures that suggest the cybercriminals do in fact possess all or most of the data maintained by Defendant in its IT systems.

38. On August 8, 2024, some portion of the data described above was released to the Dark Web and made available to those accessing those spaces, including cybercriminals. Not all of the 6.5 Terabytes was released to the Dark Web, raising the possibility that some of the data was purchased by cybercriminals as part of the auction.

39. On August 13, 2024, Defendant, by and through Mayor Andrew Ginther, stated that the information released onto the Dark Web was either "encrypted" or "corrupted," and thus not usable by bad actors. That assertion was and is plainly false and must have been known by Defendant to be false at the time. Indeed, after news reports demonstrated its reckless falsity, Mayor Ginther partially walked back those comments.

40. Plaintiffs John Doe #1 and Jane Doe have concrete evidence that their information has indeed been delivered onto the Dark Web in a usable form.

41. Moreover, data security professionals have reviewed the information on the Dark Web and have been able to identify the PII of City of Columbus employees and citizens.[10]

42. That Defendant's spokesperson, the mayor, would make these untrue statements in an attempt to minimize the impact of this disaster in the minds of Central Ohio citizens is particularly harmful in the data breach context. At a moment when affected citizens should take

[10] *See, e.g.,* 'Confirmed: Columbus data leak affects residents, and what has been released," Feuerborn, Cleary, Beachy, NBC4 News (WCMH-TV) August 13, 2024, (https://www.nbc4i.com/news/investigates/confirmed-columbus-data-leak-affects-residents-and-what-has-been-released/) (last accessed August 15, 2024).

affirmative steps to protect themselves (as Defendant itself specifically advised Columbus police officers and other employees to do), the mayor has told everyone else that all is well. Many citizens surely will believe the mayor's words and incorrectly think that there is no reason for them to take any steps at all. Thus, Defendant's reckless public pronouncements have ensured that the ultimate harm to class members will be even worse than it would otherwise have been.

43. Defendant breached its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

44. In its inaccurate press release congratulating itself on "thwarting" the cyberattack, Defendant represented that it "has been engaged in a methodical process to ensure that its technology systems are hardened against further breach before bringing them back online."

45. But this is too little too late, even if it is true. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

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

47. On information and belief, Defendant failed to design and structure its IT systems to limit the possible harm from a breach, including but not limited to compartmentalizing City systems so that a breach of one system will not implicate all City systems, and the PII of potentially hundreds of thousands of Columbus citizens.

48. On information and belief, Defendant failed to design and structure its IT systems to ensure that access is controlled and monitored to prevent breaches of this type and to allow the City to identify the source and circumstances of the breach.

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

50. Because of Defendant's Data Breach, the sensitive PII of Plaintiffs and Class Members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class and Subclass Members.

51. Upon information and belief, the cybercriminals in question are particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems, and (2) gained actual access to sensitive data.

52. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[11]

53. As clearly set forth in the materials referenced above, Class Members' Data is in fact on the Dark Web and is available to the highest bidder.

Plaintiffs' Experiences and Injuries

Plaintiffs John Doe #1 and John Doe #2

54. Plaintiffs John Doe #1 and John Doe #2 are Columbus Police Officers who have dedicated years of service to the community.

55. Defendant obtained and maintained Plaintiffs John Doe #1 and John Doe #2's PII as part of Plaintiffs' employment.

---

[11] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

56. As a result, John Doe #1 and John Doe #2 were injured by Defendant's Data Breach.

57. Other than the communications received via CPD channels, Plaintiffs John Doe #1 and John Doe #2 have received no direct communications from Defendant regarding the nature of the information compromised or the actions (if any) undertaken by Defendant to mitigate the damage from this attack.

58. Plaintiff John Doe #1 has received two notifications, one from his bank and one from his credit card provider, that his social security number has been compromised and was found on the Dark Web.

59. As such, Plaintiff John Doe #1 has suffered concrete harm as a result of Defendant's breach, as his information is unquestionable available to cybercriminals for nefarious purposes.

60. In addition, John Doe #1 and John Doe #2 have spent—and will continue to spend—significant time and effort monitoring their accounts to protect themselves from identity theft. After all, Defendant directed Plaintiffs to take those steps in its breach notice.

61. Plaintiffs John Doe #1 and John Doe #2 fear for their personal financial security and worry about what information was exposed in the Data Breach.

62. Moreover, as law enforcement officers, John Doe #1 and John Doe #2 have a particularized concern that their information will be identified and targeted by criminals to disrupt law enforcement activities and/or to threaten or intimidate Plaintiffs' family members.

63. In particular, Plaintiff John Doe #2 is an undercover officer. He has a well-founded fear that, should his identity as a police officer come to light, not only will ongoing criminal investigations be jeopardized, but his life would be in danger.

Plaintiff Jane Doe

64. Plaintiff Jane Doe is a resident of the City of Columbus. She has never been an employee of Defendant.

65. On or about October 27, 2015, Plaintiff Jane Doe entered City Hall. As part of the security procedures in place at City Hall, she presented her driver's license for scanning. Plaintiff has no choice but to provide this information to Defendant in order to access buildings to which she is entitled to access as a citizen and resident of the City of Columbus.

66. On information and belief, the information from her scanned driver's license, including driver's license number, date of birth, and expiration date, was entered into Defendant's IT database. This information was apparently maintained by Defendant from October 2015 to the present day.

67. Plaintiff Jane Doe maintains credit monitoring services that scour the Dark Web for her personal information.

68. On or about August 14, 2024, Plaintiff Jane Doe's credit monitoring service alerted her that Plaintiff Jane Doe's name, address, email, phone number, and social security number have appeared on the Dark Web.

69. On information and belief, and as a result of counsel's investigation, Plaintiff Jane Doe's information, including at a minimum stemming from her 2015 visit to City Hall, was released to the Dark Web as a result of Defendant's data breach.

70. As such, Plaintiff Jane Doe has suffered concrete harm as a result of Defendant's breach, as her information is unquestionably available to cybercriminals for nefarious purposes

71. As a result, Plaintiff Jane Doe was injured by Defendant's Data Breach.

72. Plaintiff Jane Doe fears for her personal financial security and worries about what additional information was exposed in the Data Breach.

All Plaintiffs

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

74. Plaintiffs suffered actual injury from the exposure and theft of their PII—which violates their rights to privacy.

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

76. Plaintiffs suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiffs' PII directly into the hands of criminals.

77. Because of the Data Breach, Plaintiffs anticipate spending considerable amounts of time and money to try and mitigate their injuries.

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

79. Today, Plaintiffs have a continuing interest in ensuring that their PII—which, upon information and belief, remains in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiffs and the Proposed Class and Subclass Face Significant Risk of Continued Identity Theft

80. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class Members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

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

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

h. continued risk to their PII—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

81. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

82. The value of Plaintiffs and Class's PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "Dark Web"—further exposing the information.

83. In this particular case, Plaintiffs and the Class's PII is available on the Dark Web, as demonstrated by the posts auctioning the data.

84. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

85. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

86. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

87. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this

Court or a jury, to find that Plaintiffs and other Class Members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

88. Defendant disclosed the PII of Plaintiffs and Class Members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and Class Members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

89. Defendant's failure to promptly and properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

90. Indeed, Defendant's spokesperson, the mayor, has minimized the incident and spread falsehoods about it at every turn, causing any citizen who might believe what he says to assume that they need take no action to protect themselves.

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

91. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

92. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[12] Those 330 reported breaches exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed

[12] *See 2021 Data Breach Annual Report,* IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

nearly 10 million sensitive records (9,700,238) in 2020.[13]

93. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[14]

94. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to municipalities, like Defendant.

Defendant Failed to Follow FTC Guidelines

95. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

96. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[15] The FTC declared that, *inter alia*, businesses must:

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;

---

[13] *Id*.

[14] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware.

[15] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

97. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

98. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

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

100. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former employees' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

101. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all

employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

102. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

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

104. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

105. Plaintiffs bring this class action under Ohio Civ. R. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following Class ("the Class"):

> All persons whose PII was released and compromised in the Data Breach occurring on or before July 18, 2024.

106. In addition, Plaintiffs John Doe #1 and John Doe #2 brings this class action under Ohio Civ. R. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following Subclass ("the Subclass"):

> All employees of the City of Columbus (including Franklin County Municipal Court Judges, employees of those Judges, and employees of the Franklin County Municipal Court Clerk's Office) whose PII was compromised in the Data Breach occurring on or before July 18, 2024.

107. Excluded from the Class and Subclass are Defendant, and any Judge who adjudicates this case, including their staff and immediate family.

108. Plaintiffs reserve the right to amend the class and subclass definition.

109. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

110. Ascertainability. All members of the proposed Class and Subclass are readily ascertainable from information in Defendant's custody and control. All Class Members were individuals whose PII was provided to Defendant, and all Subclass Members are or were employed by Defendant. Thus Defendant has comprehensive records of all individuals encompassed by the Class and Subclass.

111. Numerosity. The Class and Subclass Members are so numerous that joinder of all Class Members is impracticable. According to its website, the City of Columbus employs "over 10,000 people."[16] In addition, the number of former employees and citizens is several orders of magnitude larger.

[16] www.columbus.gov/Government/Jobs/WorkWithUS#:~:text=The%20City%20of%20Columbus%3A%20Your,approximately%20650%2B%20different%20job%20titles (last accessed August 6, 2024).

112. Typicality. Plaintiffs' claims are typical of the claims of the Class and Subclass as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

113. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class Members' interests. And Plaintiffs have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

114. Commonality and Predominance. Plaintiffs' and the Class and Subclass's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class and Subclass's PII;

b. if Defendant maintained a consistent policy with regard to safeguarding Plaintiffs' and the Class and Subclass's PII;

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

d. if Defendant was negligent in maintaining, protecting, and securing PII;

e. if Defendant was grossly negligence in maintaining, protecting and securing PII;

f. if Defendant breached contract promises to safeguard Plaintiffs and the Class and Subclass's PII;

g. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

h. if the Data Breach caused Plaintiffs and the Class and Subclass injuries;

i. what the proper damages measure is; and

j. if Plaintiffs and the Class and Subclass are entitled to damages and or injunctive relief.

115. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class and Subclass Members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class and Subclass Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence/Recklessness
(On Behalf of Plaintiffs and the Class and Subclass)

116. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

117. Plaintiffs and the Class and Subclass entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for appropriate operational purposes only, and/or not disclose their PII to unauthorized third parties.

118. Defendant owed a duty of care to Plaintiffs and Class and Subclass Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

119. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class and Subclass could and would suffer if their PII was wrongfully disclosed.

120. Defendant owed these duties to Plaintiffs and Class and Subclass Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's recklessly inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs and Class Members' PII.

121. Defendant owed—to Plaintiff and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their PII.

122. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff and Class and Subclass Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class and Subclass Members to take appropriate

measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

123. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

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

125. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class and Subclass. That special relationship arose because Plaintiff and the Class and Subclass entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

126. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII.

127. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and Class and Subclass Members' and the importance of exercising reasonable care in handling it.

128. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

129. Defendant breached these duties as evidenced by the Data Breach.

130. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class and Subclass Members' PII by:

a. disclosing and providing access to this information to third parties; and

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

131. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and Class and Subclass Members which actually and proximately caused the Data Breach and Plaintiffs and Class and Subclass Members' injury.

132. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class and Subclass Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and Class and Subclass Members' injuries-in-fact.

133. Defendant has admitted that the PII of Plaintiffs and the Class and Subclass was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

134. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class and Subclass Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

135. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

136. Defendant's breach of its common-law duties to exercise reasonable care and its failures, negligence, and recklessness actually and proximately caused Plaintiffs and Class and Subclass Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Negligence *per se*
(On Behalf of Plaintiffs and the Class and Subclass)

137. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

138. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class and Subclass Members' PII.

139. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the Class and Subclass Members' sensitive PII.

140. Defendant breached its respective duties to Plaintiffs and Class and Subclass Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

141. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards as

described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

142. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Members of the Class and Subclass.

143. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiffs and Class and Subclass Members would not have been injured.

144. The injury and harm suffered by Plaintiffs and Class and Subclass Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class and Subclass to suffer the foreseeable harms associated with the exposure of their PII.

145. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

146. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class and Subclass Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs John Doe #1 and John Doe #2 and the Subclass)

147. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

148. Plaintiffs and Subclass Members either directly contracted with Defendant or Plaintiff and Subclass members were the third-party beneficiaries of contracts with Defendant.

149. Plaintiffs and Subclass Members were required to provide their PII to Defendant as a condition of working for Defendant. Plaintiffs and Subclass Members provided their PII to Defendant or its third-party agents in exchange for its employment opportunities.

150. Plaintiffs and Subclass Members reasonably understood that a portion of the funds they (or their insurance carrier third-party agents) paid Defendant would be used to pay for adequate cybersecurity measures.

151. Plaintiffs and Subclass Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

152. Plaintiffs and the Subclass Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for medical services.

153. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Subclass Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

154. After all, Plaintiffs and Subclass Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

155. Plaintiffs and the Subclass fully performed their obligations under the implied contracts with Defendant.

156. The covenant of good faith and fair dealing is an element of every contract. Thus, 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—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

158. Defendant materially breached the contracts it entered with Plaintiffs and Subclass Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

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

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

160. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Subclass Members' injuries (as detailed *supra*).

161. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

162. Plaintiffs and Subclass Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

FOURTH CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiffs and the Class and Subclass)

163. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

164. Plaintiffs and the Class and Subclass had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

165. Defendant owed a duty to its current and former patients, including Plaintiffs and the Class and Subclass, to keep this information confidential.

166. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class and Subclass Members' PII is highly offensive to a reasonable person.

167. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class and Subclass disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class and Subclass were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

168. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class and Subclass's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

169. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

170. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class and Subclass in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

171. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class and Subclass.

172. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class and Subclass to suffer damages (as detailed *supra*).

173. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

174. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class and Subclass since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

175. Plaintiffs and the Class and Subclass have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class and Subclass.

176. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class and Subclass Members, also seeks compensatory damages for Defendant's invasion of

privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

FIFTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class and Subclass)

177. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

178. Given the relationship between Defendant and Plaintiffs and Class and Subclass Members, where Defendant became guardian of Plaintiffs' and Class and Subclass Members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs and Class and Subclass Members' PII; (2) to timely notify Plaintiffs and Class and Subclass Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

179. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class and Subclass Members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

180. Because of the highly sensitive nature of the PII, Plaintiffs and Class and Subclass Members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

181. Defendant breached its fiduciary duties to Plaintiffs and Class and Subclass Members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class and Subclass Members' PII.

182. Defendant also breached its fiduciary duties to Plaintiffs and Class and Subclass Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

183. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class and Subclass Members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class and Subclass, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class and Subclass;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class and Subclass;

D. Awarding Plaintiffs and the Class and Subclass damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiffs and the Class and Subclass in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiffs and the Class and Subclass leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

Respectfully submitted,

/s/ Rex H. Elliott

Rex H. Elliott (0054054)
Spencer C. Meador (0099990)
COOPER ELLIOTT
305 West Nationwide Boulevard
Columbus, Ohio 43215
(614) 481-6000
(614) 481-6001 (Facsimile)
rexe@cooperelliott.com
spencerm@cooperelliott.com

Matthew R. Wilson (0072925)
Michael J. Boyle, Jr. (0091162)
Jared W. Connors (0101451)
MEYER WILSON CO, LPA
305 West Nationwide Boulevard
Columbus, Ohio 43215
(614) 224-6000
(614) 224-6066 (Facsimile)
mwilson@meyerwilson.com
mboyle@meyerwilson.com
jconnors@meyerwilson.com

Attorneys for Plaintiffs
and Proposed Class

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

/s/ Rex H. Elliott