IN THE COURT OF COMMON PLEAS
FRANKLIN COUNTY, OHIO

JOHN DOES #1-8 c/o Counsel Arnold & Clifford LLP 115 W. Main St., Fourth Floor Columbus, OH 43215	:	Case No. _____
	:	Judge _____
and	:	
JANE DOE #1 c/o Counsel Arnold & Clifford LLP 115 W. Main St., Fourth Floor Columbus, OH 43215	:	**JURY DEMAND ENDORSED HEREON**
Plaintiffs,	:	
v.	:	
CITY OF COLUMBUS c/o Columbus City Attorney 77 North Front Street Columbus, OH 43215	:	
Defendant.	:	

CLASS ACTION COMPLAINT

Now come Plaintiffs John Does 1-8 and Jane Doe 1 ("Plaintiffs"), individually and on behalf of all others similarly situated, and bring their Class Action Complaint against Defendant the City of Columbus ("City" or "Defendant") and hereby state:

INTRODUCTION

1. Defendant failed to comply with industry standards to protect information systems that contain personal identifiable information ("PII"). As a result, on or about July 18, 2024, Defendant was the target of a ransomware cyberattack on its information technology ("IT") system, resulting in the theft of PII belonging to Plaintiffs' and the proposed class defined below

(referred to as the "Class" or "Class Members"). Plaintiffs bring this class action against Defendant for its failure to properly secure the PII of Plaintiffs and members of the proposed Class.

2. The PII includes, among other things, Plaintiffs' names, addresses, birth dates, driver's license numbers, Social Security numbers, and financial account information.

3. Plaintiffs seek, among other things, orders requiring Defendant to fully and accurately disclose the nature of the information that has been compromised and to adopt sufficient security practices and safeguards to prevent incidents like the data breach described herein in the future. Plaintiffs also seek reimbursement of their actual losses, compensatory and punitive damages, attorney fees, all costs associated with reclaiming and protecting their identities, and monitoring costs.

4. On July 29, 2024, Defendant boasted that it had "thwarted" the attempt of "a foreign cyber threat actor" to disrupt the City's IT infrastructure. Shortly thereafter, however, current and former employees of the City, including employees of the Columbus Police Department ("CPD") and the Columbus Fire Department ("CFD"), reported to the City that they were victims of fraudulent transactions, that they were alerted to attempted illicit uses of their PII on the dark web, and that their information was now present on the dark web as a result of the City being hacked.

5. Despite these reports, on August 13, 2024, Mayor Ginther (the "Mayor") held a news conference in which he told reporters that "the data stolen during the ransomware attack on the city was corrupted or likely unusable." The Mayor's assertion was quickly contradicted by a cybersecurity expert who located some of the data stolen from the City that was available on the dark web.

6. Defendant knowingly requests and obtains sensitive PII and has a duty to securely maintain that information in confidence.

7. Plaintiffs seek to remedy these harms individually and on behalf of all other similarly situated individuals whose PII was exposed in the data breach.

PARTIES

8. John Doe 1 is an individual who is employed by the City and serves as a member of the CPD.

9. John Doe 2 is an individual who is a retired member of the CPD.

10. John Doe 3 is an individual who is a former member of the CPD.

11. Jane Doe 1 is an individual who is employed by the City and serves as a member of the CPD.

12. John Doe 4 is an individual who currently is employed by the City and serves as a member of the CPD.

13. John Doe 5 is an individual who currently is employed by the City and serves as a member of the CPD.

14. John Doe 6 is an individual who currently is employed by the City and serves as a member of the CPD.

15. John Doe 7 is an individual who is a retired member of the CPD..

16. John Doe 8 is an individual who currently is employed by the City and serves as a member of the CFD.

17. Defendant City of Columbus is a municipal corporation under R.C. 703.1(A).

JURISDICTION AND VENUE

18. Jurisdiction may be exercised over Defendant under R.C. 2305.01 and R.C. 2307.382(A)(1) and (3) because Defendant transacted business in Ohio and caused tortious injury by an act or omission in Ohio.

19. Venue is proper in this Court under Ohio Civil Rule 3(C)(2), (3), and/or (6) because Franklin County is the county in which (a) Defendant (a municipal corporation) has its principal place of business, (b) Defendant conducted activity that gave rise to the claims raised in the Complaint, and/or (c) all or part of the claims for relief arose there.

20. The City's actions described herein are Proprietary Activities under R.C. 2744.01(G)(1) and not governmental activity under R.C. 2744.01(C)(1)(a), 2744.01(C)(1)(b), or 2744.01(C)(2). The City's actions are 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." Under R.C. 2744.02(B)(2), the City is "liable for injury, death, or loss to person or property caused by the negligent performance of acts by [its] employees" for its actions described in this Complaint.

FACTUAL ALLEGATIONS

The Ransomware Attack

21. The City employs over 10,000 people. One of the City's departments is the Department of Technology ("DOT"). The DOT's website states that its "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. DOT does this 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."

22. The DOT's website further provides that the department's leaders "help inspire approximately 185 dedicated technology employees who work tirelessly to support City

departments and promote the critical importance of digital equity and inclusion, open data, and tools that help keep Columbus residents safe and informed."

23. Noticeably absent from the DOT's description of its mission and work is the safeguarding of the PII in the City's IT system.

24. The City's IT system holds electronic records for virtually all City operations, including those of the CPD and CFD.

25. The City receives and stores the PII of thousands of its current employees, former employees, family members of current and/or former employees, and private citizens.

26. On or about July 18, 2024, the City experienced a computer outage that was later revealed to be a cybersecurity incident.

27. On July 29, 2024, Defendant released a press release titled "Columbus Thwarted Ransomware Encryption of its IT Infrastructure" and 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. Fortunately, the city's Department of Technology quickly identified the threat and took action to significantly limit potential exposure, which included severing internet connectivity. While the threat actor's activity was disrupted, an investigation is ongoing to determine the amount of city data potentially accessed."[1]

28. On or about July 31, Rhysida, an international ransomware group, listed stolen Columbus city government data as being up for sale on the group's website on the dark web.[2] Rhysida reportedly "stole more than 6.5 terabytes of databases, internal logins and passwords of employees, along with 'a full dump of servers with emergency service applications of the city' and

[1] https://www.columbus.gov/News-articles/City-of-Columbus-Thwarted-Ransomware-Encryption-of-its-IT-Infrastructure, last accessed August 17, 2024.

[2] https://www.dispatch.com/story/news/local/2024/08/01/rhysida-ransomware-group-says-its-behind-columbus-cyberattack/74629627007/, last accessed August 16, 2024.

'access from city video cameras.'" *Id.* The group reportedly was "asking for 30 bitcoin, or around $1.9 million, as payment for the stolen data." *Id.*

29. On August 1, 2024, the City informed its employees that they would receive two years of free credit monitoring services.

30. As of August 7, 2024, it appeared that Rhysida had not received its asking price for the data stolen from the City and released the City's data making it publicly available to users on the dark web.[3]

31. On the morning of August 13, 2024, the Mayor held a press conference in which he told reporters that "the data stolen during the ransomware attack on the city was corrupted or likely unusable."[4]

32. However, contrary to the Mayor's statements, a cybersecurity expert reportedly went onto the dark web and analyzed the stolen data. *Id.* That individual reportedly "found the names, addresses, birth dates, driver's license numbers, and Social Security numbers of more than 470,000 people in Columbus and outside of the state of Ohio." *Id.* The data included "the names of domestic violence and sexual assault victims and juveniles who are either victims or suspects in crimes" and "the names of people who visited city hall." *Id.*

Municipalities are Primary Targets for Ransomware Attacks

33. Prior to the July 18, 2024 attack on its IT system, the City knew or should have known about the threat of a ransomware attack on its IT system because ransomware attacks on municipal IT systems have plagued municipalities for many years.

---

[3] https://www.dispatch.com/story/news/local/2024/08/07/rhysida-threatens-to-release-stolen-columbus-data-unless-ransom-paid/74705811007/ , last accessed August 16, 2024.

[4] https://www.dispatch.com/story/news/local/2024/08/13/cybersecurity-expert-connor-goodwolf-says-data-of-private-citizens-stolen-in-columbus-cyberattack/74789870007/ , last accessed on August 16, 2024.

34. For example, over six years ago, in March 2018, the city of Atlanta was the target of a ransomware attack.[5] The 2018 ransomware attack on Atlanta caused significant disruption to the city's operations and reportedly resulted in the loss of decades' worth of city council correspondence. *Id.* At the time, it was reported that Atlanta had "a lax approach toward cybersecurity" and a lesson from the incident was that "Government IT officials might find it's better to spend more money up front hardening their cybersecurity, rather than shelling out after a hack." *Id.*

35. In the years since the 2018 ransomware attack on Atlanta, multiple municipalities have been the target of ransomware attacks. In May 2019, Baltimore was the target of a ransomware attack, which reportedly cost the city $18 million in recovery expenses.[6] In late 2019, New Orleans was the target of a ransomware attack. *Id.*

36. In May 2023, the city of Dallas was the target of a ransomware attack affecting, among other things, police, utility, and court systems. *Id.* For the Dallas attack, "a ransomware group threatened to release sensitive information it had accessed, including employee information, medical information, and detailed court records." *Id.* It is not clear whether Dallas paid the ransom, but reportedly "Dallas City Council later signed off on an $8.5 million bill, including money for vendors who helped in the recovery process." *Id.*

37. As recently as June 2024, the city of Cleveland responded to a cyber "threat." *Id.*

38. Additionally, a report from the Center for Internet Security "found that malware attacks on state and local governments more than doubled between 2022-2023."[7]

---

[5] See https://statescoop.com/atlanta-was-not-prepared-to-respond-to-a-ransomware-attack/, last accessed August 15, 2024.

[6] Ransomware attacks cost cities millions. Will Cleveland face the same fate? - cleveland.com, last accessed August 16, 2024.

[7] https://www.axios.com/local/columbus/2024/08/16/ohio-cyberattack-rhysida-data-leak, last accessed August 16, 2024.

The City's Failure to Properly Secure the PII in its Possession Caused, and will Continue to Cause, Plaintiffs to Suffer Identity Theft and Financial Loss

39. Thus, from over a half-decade worth of examples of cyberattacks on municipalities, it should have been clear to the City (of Columbus) that it was not immune to cyberattacks and a municipality's failure to implement sufficient cybersecurity measures would result in serious consequences affecting its citizens, employees, and anyone who entrusted his or her PII with the City.

40. The City did not heed the cautionary tales of attacks on other municipalities. The City's efforts to protect the PII in its possession, if any, were woefully inadequate.

41. As early as July 29, 2024 (the same day as the City's press release that it "Thwarted Ransomware Encryption of its IT Infrastructure"), John Doe 1's bank account had unauthorized purchases from big box retailers, and he received a text message stating that his information was leaked in a security breach and if he did not pay $500 by midnight then the officer's information would be released on the dark web.

42. As of August 2024, John Doe 2 had received reports that his personal information was stolen as part of the data breach.

43. On August 2, 2024, John Doe 3's checking account was accessed and over a thousand dollars was fraudulently withdrawn from his account.

44. In August 2024, Jane Doe 1 was advised that someone attempted to make fraudulent online purchases using her credit card that was linked to her online account.

45. In late July 2024, after learning about the data breach, John Doe 4 spent multiple hours on the phone and made multiple trips to his bank to ensure that any of his stolen data would not be used. He opened new accounts and transferred funds, which required him to purchase new checks. He also purchased data protection services.

46. In August 2024, John Doe 5 discovered fraudulent transactions from his bank account caused by the data breach.

47. In August 2024, John Doe 6 learned that, following the data breach, unknown individuals were attempting to take out loans in his name.

48. In mid-August 2024, John Doe 7 was informed that his name, social security number, email address, date of birth, phone number, and address were all available on the dark web.

49. In August 2024, John Doe 8 was advised that his social security number was located on the dark web.

50. Plaintiffs have had to expend substantial time addressing alerts and notifications of activity associated with the ransomware attack. Plaintiffs have also suffered from increased stress and anxiety as a direct result of the financial uncertainty caused by the ransomware attack. Under Ohio law, police officer residential and familial information is exempt from public disclosure. As a direct result of the ransomware attack upon the City's IT system, police officers' home addresses have been disclosed, and officers now worry about criminals discovering where they live and visiting their families while they are working.

51. These incidents are a direct result of the City's inadequate efforts to protect PII in its possession. Moreover, virtually all of the incidents predate Mayor Ginther's false statement that "the data stolen during the ransomware attack on the city was corrupted or likely unusable." Not only has the City shown that it could not be trusted with the PII in its possession, but it also cannot be trusted to remedy the harm it caused.

CLASS ALLEGATIONS

52. Plaintiffs incorporate each and every allegation contained in the preceding paragraphs by reference as if fully set forth herein.

53. Plaintiffs, in accordance with Rule 23(B) of the Ohio Rules of Civil Procedure, bring this action on behalf of themselves and as a member of the Class defined below.

54. Plaintiffs seek to represent a Class comprised of all current and former employees of the City of Columbus, and the spouses, children, or other dependents of current and former employees of the City of Columbus, whose PII was electronically stored by the City of Columbus as of July 18, 2024.

55. The following are excluded from the Class: (a) any Judge or Magistrate presiding over this action and members of their families and (b) all persons who properly execute and file a timely request for exclusion from the Class.

56. The Class is so numerous that joinder of all members is impracticable.

57. There are questions of law and fact common to the Class. These common questions include, but are not limited to, whether Defendant failed to adequately protect the PII in its possession from cybertheft in violation of federal and state law.

58. The claims of Plaintiffs, which arise out of Defendant's failure to adequately protect the PII in its possession from cybertheft, are typical of the claims of the Class members. Likewise, Defendant's defenses to Plaintiffs' claims would be typical of the defenses to the Class claims.

59. Plaintiffs will fairly and adequately represent and protect the interest of the Class. Plaintiffs are articulate and knowledgeable about their claims and fully able to describe them. There are no conflicts of interest between Plaintiffs with respect to the interests of the Class members. Plaintiffs, like the Class members, have suffered financial loss as a result of Defendant's

acts. Plaintiffs have sufficient financial resources to litigate this case and further the interests of the Class without compromising them.

60. Counsel for Plaintiffs are well-suited to represent their interests and the interests of the Class at large. Counsel includes James E. Arnold, Gerhardt A. Gosnell, Damion M. Clifford, and Damien Kitte of Arnold & Clifford, LLP, and Scott Schiff and Zach Schiff of Schiff & Associates. The combined experience and areas of professional concentration of these attorneys are well-suited to representation of the interests of the Class. The Arnold & Clifford lawyers all practice complex civil litigation and are experienced in class action litigation.

61. Class certification is appropriate pursuant to Rule 23(B)(1) of the Ohio Rules of Civil Procedure. Prosecuting separate actions would create a risk of adjudications with respect to individual Class members that, as a practical matter, would be dispositive of the interests of the other members not parties to the individual adjudications or would substantially impair or impede their ability to protect their interests.

62. Class certification is appropriate under Rule 23(B)(2) of the Ohio Rules of Civil Procedure. Defendant will continue to commit the alleged violations, and the members of the Class will continue to suffer from inadequate protection of their PII. Defendant has acted and refused to act on grounds that apply generally to the Class so that final injunctive relief is appropriate with respect to the Class as a whole.

63. Class certification is appropriate under Rule 23(B)(3) of the Ohio Rules of Civil Procedure. The questions of law or fact common to the members of the Class, described above, predominate over any questions affecting only individual members.

64. This Court is an appropriate forum for the litigation of the Class claims.

COUNT 1 – Negligence (on behalf of Plaintiffs and the Class)

65. Plaintiffs reallege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

66. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' PII, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. That duty included, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs' and Class Members' PII in Defendant's possession was adequately secured and protected, that Plaintiffs' and Class Members' PII on Defendant's networks were not accessible to criminals, and that Defendant employees tasked with maintaining such information were adequately trained on security measures regarding the security of Plaintiff's and Class Members' PII.

67. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

68. Plaintiffs and Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information, use their PII for municipal business purposes only, and not disclose their PII to unauthorized third parties.

69. Defendant knew or reasonably should have known that a failure to exercise due care in collecting, storing, and using Plaintiffs' and Class Members' PII involved an unreasonable risk of harm to Plaintiffs and Class Members.

70. Upon information and belief, Defendant's inadequate practices with respect to safeguarding Plaintiffs' and Class Members' PII was wanton, willful, or with a reckless disregard

toward the harm that could befall Plaintiffs and the Class Members in the event of a ransomware attack.

71. A breach of cybersecurity, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable to Defendant, particularly in light of prior data breaches and disclosures experienced by other municipalities.

72. Plaintiffs and the Class Members were the foreseeable and probable victims of any of Defendant's inadequate cybersecurity practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Plaintiffs' and Class Members' PII.

73. Defendant unlawfully breached its duties to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' PII within its possession.

74. As a direct and proximate cause of Defendant's breach of its duties owed to Plaintiffs and the Class Members, the Plaintiffs and Class Members have suffered damages in an amount to be determined at trial.

75. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to PII; and (2) compelling Defendant to provide detailed and specific disclosure of what types of PII have been compromised as a result of the data breach.

COUNT 2 – Negligence *Per Se* (on behalf of Plaintiffs and the Class)

76. Plaintiffs reallege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

77. Under the Federal Trade Commission Act ("FTC Act"), 15 U.C.S. § 45, "unfair … practices in or affecting commerce, are … unlawful."

78. The failure of an entity such as a municipal corporation to reasonably protect PII in its possession constitutes an unfair practice under the FTC Act. Reasonable protection of PII in its protection is a duty imposed upon Defendant by the FTC Act.

79. Defendant violated the FTC Act by failing to comply with applicable industry standards with respect to the protection of Plaintiffs' and the Class Members' PII in Defendant's possession.

80. Defendant thus breached its duty under the FTC Act by failing to employ industry standard data and cybersecurity measures to reasonably protect Plaintiffs' and the Class Members' PII in its possession.

81. It was reasonably foreseeable, particularly given the growing number of data breaches of municipalities, that the failure to reasonably protect and secure Plaintiffs' and Class Members' PII would result in an unauthorized third-party gaining access to Defendant's IT system that stored or contained Plaintiffs' and the Class Members' PII.

82. Defendant's violations of the FTC Act constitute negligence *per se*.

83. Plaintiffs and the Class Members are within the category of persons the FTC Act was intended to protect.

84. The harm that occurred as a result of the data breach is the type of harm the FTC Act was intended to guard against.

85. Plaintiffs' and the Class Members' PII constitute personal property that was stolen due to Defendant's negligence, resulting in harm, injury and damages to Plaintiffs and the Class Members.

86. As a direct and proximate cause of Defendant's breach of its duties owed to Plaintiffs and the Class Members under the FTC Act, Plaintiffs and the Class Members have suffered damages in an amount to be determined at trial.

87. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to PII; and (2) compelling Defendant to provide detailed and specific disclosure of what types of PII have been compromised as a result of the data breach.

COUNT 3 – Breach of Contract

88. Plaintiffs reallege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

89. At the time of entering employment with Defendant, Plaintiffs and the Class Members entered into a contractual relationship with Defendant.

90. A condition of employment was that Plaintiffs and the Class Members were to provide Defendant with their PII.

91. Defendant was obligated to safeguard Plaintiffs' and the Class Members' PII and use adequate cybersecurity procedures with respect to safeguarding Plaintiffs' and the Class Members' PII.

92. Defendant breached its contractual relationship with Plaintiffs and Class Members by failing to use adequate cybersecurity procedures with respect to safeguarding Plaintiffs' and the Class Members' PII.

93. Plaintiffs and the Class Members have performed all obligations under their contractual relationship with Defendant and/or their obligations have been waived.

94. As a direct and proximate cause of Defendant's breach of its contractual obligations, Plaintiffs and the Class Members have suffered damages in an amount to be determined at trial.

95. Plaintiffs seek injunctive relief on behalf of the Class in the form of an order (1) compelling Defendant to institute appropriate data collection and safeguarding methods and policies with regard to PII; and (2) compelling Defendant to provide detailed and specific disclosure of what types of PII have been compromised as a result of the data breach

WHEREFORE, Plaintiffs and the Class request the following relief:

(1) An Order certifying this action as a class action, pursuant to Rule 23 of the Ohio Rules of Civil Procedure, designating Plaintiffs John Does 1-8 and Jane Doe 1 as the Class representatives, and designating counsel for Plaintiffs as Class Counsel

(2) Injunctive relief requiring the Defendant to fully and accurately disclose the information that has been compromised, to provide data monitoring services, at no charge, to Plaintiffs and the Class for a period of 5 years, and to adopt sufficient security practices and safeguards to prevent incidents like the data breach described in this Complaint in the future;

(3) Award damages, including compensatory, exemplary, punitive, and statutory damages, to Plaintiffs and the Class in an amount to be determined at trial, for the acts complained of herein;

(4) Award Plaintiffs and the Class their expenses and costs of suit, including reasonable attorneys' fees to the extent provided by law;

(5) Award Plaintiffs and the Class pre-judgment and post-judgment interest;

(6) All other and further relief to which Plaintiffs and the Class are entitled by law or in equity as may be determined by the Court to be just, equitable, and proper.

Respectfully submitted,

/s/ Damion M. Clifford
James E. Arnold (0037712)
Damion M. Clifford (0077777)
Gerhardt A. Gosnell II (0064919)
Damien C. Kitte (0084057)
ARNOLD & CLIFFORD, LLP
115 West Main Street, Fourth Floor
Columbus, Ohio 43215
Telephone: (614) 460-1600
Facsimile: (614) 469-1134
Email: jarnold@arnlaw.com
dclifford@arnlaw.com
ggosnell@arnlaw.com
dkitte@arnlaw.com

Scott W. Schiff (0033745)
Zachary L. Schiff (0095628)
Schiff & Associates Co., L.P.A.
115 West Main Street, Suite 100
Columbus, Ohio 43215
Telephone: (614) 621-8888
Facsimile: (614) 621-8814
Email: scott@schifflegal.com
zschiff@schifflegal.com

Attorneys for Plaintiffs

JURY DEMAND

Plaintiffs hereby demand a trial by jury on all counts of their Complaint so triable.

/s/ Damion M. Clifford
Damion M. Clifford