IN THE COURT OF COMMON PLEAS
FOR FRANKLIN COUNTY, OHIO

JOHN DOE #1, et al., on behalf of themselves and all others similarly situated, Plaintiffs, v. CITY OF COLUMBUS, Defendant.	Case Nos. 24CV6195 and 24CV6428 Judge Carl Aveni

PLAINTIFFS' MEMORANDUM IN OPPOSITION
TO DEFENDANT'S MOTION TO DISMISS

TABLE OF CONTENTS

INTRODUCTION

The City's motion to dismiss rests on a series of outlandish propositions. In the City's view, it has no duty to safeguard the highly sensitive, personally identifying information (PII) it collected from its employees and citizens. And although millions of employees' and residents' PII has been posted on a dark web forum frequented by identity thieves, the City says there is no real risk of identity theft. Perhaps most shockingly of all, the City even claims that undercover police officers are not harmed by the public disclosure of their identities.

Not even the City believes any of that is true. After the City wrongly claimed to have "thwarted" the data breach, and following Mayor Andrew Ginther's erroneous declaration that none of the information posted on the dark web could be used by bad actors, a dark web researcher used that publicly available data to correct the City's dangerous misrepresentations and assist the public. In response, the City rushed to the courthouse to silence him, filing a lawsuit seeking damages and injunctive relief for claims such as negligence and invasion of privacy—two of the very claims that the City now says are not available to the actual victims of the data breach. *See City of Columbus v. Ross*, No. 24CV006703 (Franklin C.P. Aug. 29, 2024). In support of the City's widely criticized[1] motion for a temporary restraining order, numerous city officials submitted

[1] *See, e.g.*, Open Letter to Columbus City Attorney Zach Klein from Information Security Professionals (Sep. 10, 2024), https://disclose.io/uploads/open_letter_columbus_attorney_zach_klein.pdf; Kevin Williams, *Dark web researcher warned Columbus, Ohio, residents ransomware attack was bigger than mayor said. The city is suing him*, CNBC (Sep. 15, 2024), https://www.cnbc.com/2024/09/15/dark-web-expert-warned-us-hometown-about-big-hack-the-city-is-suing.html (quoting Kyle Hanslovan, CEO of cybersecurity company Huntress: "In this case, it appears we have just silenced someone who, as far as I can tell, appears to be a security researcher who did the bare minimum and confirmed the official statements made were not true. This can't possibly be an appropriate use of the courts."); Amelia Robinson, *My info was stolen in the Columbus cyberattack. It is ridiculous the city is targeting cyber expert*, COLUMBUS DISPATCH (Aug. 30, 2024), https://www.dispatch.com/story/opinion/columns/2024/08/30/columbus-dark-web-connor-goodwolf-randomware-restraining-order-against/75001552007/.

sworn affidavits attesting to the seriousness of the data breach and the grave risk of harm it presented for the victims:

- **Police Chief Elaine Bryant** stated that the data breach "target[ed] some of the City's most sensitive databases concerning individuals' personal information," and that the information exposed in the breach could "reveal the identities of undercover police officers, minor victims of crimes, and more." Chief Bryant further testified that if this information were publicly disclosed—which it has indeed been—there would be "a real and ongoing threat" of "irreparable harm." Exhibit A: Affidavit of Elaine Bryant.
- **Director of Technology Sam Orth** testified that the data breach was "massive" and involved "some of the City's most sensitive databases containing individuals' personal information." That information is now available on the dark web, "a place for criminals to go and use bitcoin to purchase stolen information they would use to do harm to others." Exhibit B: Affidavit of Sam Orth.
- **Deputy City Attorney Lara Baker-Morrish** said that the information posted to the dark web included "two backup databases that contain large amounts of data gathered by City prosecutors and the Columbus Division of Police," as well as "sensitive personal information of police officers." Exhibit C: Affidavit of Lara Baker-Morrish.

Perhaps the most telling statement is the City Attorney's explanation for why his office chose to file a lawsuit against a well-intentioned researcher:

> "As far as the complaint, it exists because of the City's duty to protect stolen data from dissemination, including the potential exposure of the identities of undercover police officers, evidence in ongoing criminal investigations, and sensitive personal information of residents," reads an emailed statement from the Columbus city attorney's office.

Sophia Fox-Sowell, *Columbus, Ohio's messy ransomware saga underscores legal gray areas*, STATESCOOP (Oct. 23, 2024), https://statescoop.com/columbus-ohio-ransomware-saga-legal-gray-areas-2024/.

Yet the City would now have the Court believe that it has no obligation to safeguard PII, that the information exposed in the breach presents no real risk of harm, and that the victims of the data breach—even undercover police officers—suffered no harm at all. Deep down, we all know better. The Court should deny the City's motion to dismiss.

STATEMENT OF FACTS

This case arises from a data breach. Defendant the City of Columbus collects and stores vast quantities of sensitive PII from its citizens and employees. Consolidated Amended Complaint ("CAC") ¶¶ 20–26. In 2024, hackers gained access to the City's systems and exfiltrated at least 6.5 terabytes of highly sensitive data, which they soon posted on a dark web auction house frequented by identity thieves. *Id.* ¶¶ 31–41. As a result, the sensitive PII of thousands of people has been publicly disclosed. *Id.*

The cyberattack should not have come as a surprise to the City. The PII that it stored on its servers has a high value on the secondary market, making it an enticing target for hackers. *Id.* ¶¶ 94–95. Moreover, there have been thousands of data breaches over the past several years, and many targeted municipalities like the City. *Id.* ¶¶ 104–13. Therefore, it was highly foreseeable that hackers would target the City's systems to steal Plaintiffs' PII. *Id.*

The data breach would never have occurred but-for the City's negligence. *Id.* ¶¶ 5, 150, 155, 165. The City recklessly maintained its data in a single, unified system for all City services and entities, which meant that a breach in any part of the City's system would give the hackers access to *all* of the City's data, including Plaintiffs' PII. *Id.* ¶¶ 2–3, 28, 50–51. In addition, the City's data security practices and procedures violated numerous FTC guidelines and industry best practices. *Id.* ¶¶ 114–23.

Plaintiffs are victims of the data breach who have been injured by the City's reckless conduct. *Id.* ¶¶ 6, 8–13, 86–93.

- Plaintiff John Doe #1 is a Columbus Police Officer who has dedicated years of service to the community and currently serves in an undercover role. *Id.* ¶ 57. The City obtained and maintained his PII as a condition of his employment, but his PII was exposed in the City's data breach and is now on the ark Web. *Id.* ¶¶ 58–59. He was also locked out of his bank account in mid-August 2024. *Id.* John Doe #1 fears for his personal financial security. *Id.* ¶ 64. As a law enforcement officer, John Doe #1 has a particularized concern that his information will be identified and targeted by criminals. *Id.* ¶ 65. 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. *Id.* As a result, he fears for his safety more now than ever before.

Id. ¶ 69. He sleeps with a gun under his pillow, and he has had to install security cameras throughout his home. *Id.* ¶ 69.

- In late July 2024, Plaintiff John Doe #2's bank account revealed unauthorized purchases from big box retailers, and he received a text message stating that if he did not pay a $500 ransom by midnight then his information would be released on the Dark Web. *Id.* ¶¶ 70-71.
- In late July 2024, after learning about the City's data breach, Plaintiff John Doe #3 opened new accounts and transferred funds, which required him to purchase new checks. *Id.* He also purchased data protection services. *Id.* ¶ 72.
- Following the City's data breach, Plaintiff John Doe #4 received ransom emails threatening to distribute personal information if he did not pay the sender a specified sum of money. *Id.* ¶ 73. He continues to receive ransom emails, causing him distress regarding his and his family's safety. *Id.*
- In late July 2024, Plaintiff John Doe #5 received multiple alerts that his credit card had been compromised. *Id.* ¶ 74. He was later informed that his social security number was available on the Dark Web as a result of the City's data breach and unknown individuals and entities were attempting to use that information. *Id.*
- Plaintiff Jane Doe is a resident of the City of Columbus. *Id.* ¶76. She has never been an employee of the City. *Id.* In October 2015, Jane Doe entered City Hall. *Id.* ¶ 77. As part of the procedures in place at City Hall, she presented her driver's license for scanning. *Id.* Plaintiff also paid a parking ticket with the City. *Id.* ¶ 79. In August, 2024, Jane Doe's credit monitoring service alerted her that her PII appeared on the Dark Web as a result of the City's data breach. *Id.* ¶ 81–82. Jane Doe also fears for her personal financial security. *Id.* ¶ 85.

Plaintiffs' injuries have been exacerbated by the City's incompetent response to the data breach. *Id.* ¶¶ 45, 102–03. Shortly after detecting the cyberattack, the City issued a press release, published on its website, entitled "Columbus Thwarted Ransomware Encryption of its IT Infrastructure." *Id.* ¶ 35. Unfortunately, the City did not, of course, "thwart" the cyberattack. *Id.* ¶ 36. Worse, even after the hackers had posted the data on the Dark Web, the City, through Mayor Andrew Ginther, stated that the stolen data was either "encrypted" or "corrupted," and thus not usable by bad actors. *Id.* ¶ 42. That assertion was false and must have been known by the City to be false at the time it was made. *Id.* Multiple Plaintiffs have concrete evidence that their information has indeed been delivered onto the Dark Web in a usable form. *Id.* ¶ 43. Moreover, data security professionals have reviewed the information on the Dark Web and have been able to identify City employees' and residents' PII. *Id.* ¶ 44.

That the City would make these untrue statements in an attempt to minimize the impact of this disaster in the minds of its citizens is particularly harmful in the data breach context. *Id.* ¶ 45. At a moment when affected citizens should take affirmative steps to protect themselves, the City told everyone that all is well. *Id.* The City's reckless public pronouncements have ensured that the ultimate harm to Plaintiffs will be even worse than it would have otherwise been. *Id.* Because of the City's data breach, Plaintiffs' sensitive PII was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs. *Id.* ¶ 53.

ARGUMENT

I. The City is not entitled to immunity.

The City argues incorrectly that it is immune from Plaintiffs' tort claims. "R.C. Chapter 2744 establishes a three-tiered analysis for reviewing claims of political subdivision immunity." *Scott v. City of Columbus Dept. of Pub. Util.*, 2011-Ohio-677, ¶ 7 (10th Dist.). "However, that immunity is not absolute." *Colbert v. City of Cleveland*, 99 Ohio St.3d 215, 2003-Ohio-3319, ¶ 7, citing R.C. 2744.02(B). Under the first tier, political subdivisions are "not liable in damages in a civil action for injury, death, or loss to person or property allegedly caused by any act or omission of the political subdivision or an employee of the political subdivision in connection with a governmental or proprietary function." *Scott*, 2011-Ohio-677, at ¶ 7. But the analysis does not stop there. Once immunity is established, the Court must evaluate whether one of the five exceptions to immunity under R.C. 2744.02(A) apply. *Id.* Then, "under the third tier of analysis, if one or more of the exceptions . . . apply to rid the political subdivision of immunity, the political subdivision may assert one of the affirmative defenses in R.C. 2744.03 to reinstate immunity." *Id.* Here, Plaintiffs have alleged an exception under R.C. 2744.02(B)(2), and the City cannot establish an affirmative defense under R.C. 2744.03. Thus, the City is not immune from Plaintiffs' claims.

A. R.C. 2744.02(B)(2) provides an exception to the City's immunity.

Although the City enjoys general immunity, the exception to that immunity under R.C. 2744.02(B)(2) applies in this case. Under R.C. 2744.02(B)(2), the City is liable for injury caused

by the "negligent performance of acts by their employees with respect to proprietary functions of the political subdivisions." Thus, R.C. 2744.02(B)(2) turns on whether the City's actions at issue here constitute a "proprietary function." The City argues that its actions are governmental functions, but the City is wrong. Its actions were plainly proprietary.

1. The City's maintenance of PII and confidential information on its IT system is not a government function.

The City argues that maintaining an IT System with PII and confidential information constitutes a governmental function. But the City contorts the definition of "governmental function" to suit its needs. The City cannot show that it was engaged in a governmental function.

"'Governmental function' means a function of a political subdivision that is specified in [R.C. 2744.01(C)(2)] or that satisfies any of the following: (a) A function that is imposed upon the state as an obligation of sovereignty and that is performed by a political subdivision voluntarily or pursuant to legislative requirement; (b) A function that is for the common good of all citizens of the state; (c) A function that promotes or preserves the public peace, health, safety, or welfare; that involves activities that are not engaged in or not customarily engaged in by nongovernmental persons; and that is not specified in division (G)(2) of this section as a proprietary function." R.C. 2744.01(C)(1)(a)–(c).Importantly, maintenance of an IT System with PII and confidential information is not specified under R.C. 2744.02(C)(2). Moreover, the City cannot satisfy any of the requirements of R.C. 2744.01(C)(1)(a), (b), or (c). Indeed, The City makes no effort to satisfy R.C. 2744.01(C)(1)(a). Nor could it. The City cannot show that maintaining an IT System is a function imposed upon the state as an obligation of sovereignty that is performed by a political subdivision voluntarily or pursuant to legislative requirement.

R.C. 2744.01(C)(1)(b) similarly does not apply here. The City conveniently omits the key phrase "of the state" in an attempt to shoehorn its argument into an inapplicable definition. The City argues, "The operation of the City's IT infrastructure is performed for the entire City and is a function for the common good of all citizens and therefore constitutes a government function." Mot. at 8. The statute, however, requires that the function be "for the common good ***of all citizens***

of the state." R.C. 2744.01(C)(1)(b) (emphasis added). The City cannot show that its maintenance of an IT System is for the common good for "***all citizens <u>of the state</u>***" and not just the City. *See Alcus v. Bainbridge Twp.*, 2020-Ohio-543, ¶ 115 (11th Dist.) ("***The Township's maintenance of its grounds only benefits some of the citizens of the state***, mainly Township employees who work there, and to some extent, the visitors who are permitted access, ***not all citizens of the state. Accordingly, the Township was not engaged in a governmental function under R.C. 2744.01(C)(1)(b)***.") (Emphasis added.) As a result, the City cannot show that maintaining an IT System is a government function under R.C. 2744.01(C)(1)(b).

The City also cannot earnestly argue that R.C. 2744.01(C)(1)(c) applies. Maintaining an IT System is not a "function that promotes or preserves the public peace, health, safety, or welfare; that involves activities that are not engaged in or not customarily engaged in by nongovernmental persons . . . ." *Id.* There can be no dispute that maintaining an IT System with PII and confidential information is a function customarily engaged in by almost all nongovernmental entities, as demonstrated by the many data breach cases brought against private companies.[2] Thus, the City's maintenance of an IT System is not a governmental function under R.C. 2744.01(C)(1)(c).

The City next argues that "Courts have found that functions that are 'sometimes performed by private entities for political subdivisions' do <u>not</u> qualify for an exception to immunity on that basis." Mot. at 9 (emphasis in original). The City's analysis, however, distorts relevant case law and Plaintiffs' allegations. For example, the fact that some of the government functions enumerated under R.C. 2744.01(C)(2) can sometimes be performed by private entities does not transform these functions into proprietary functions. *See Austin v. City of Warrensville Hts.*, 2021-Ohio-1950, ¶ 17 (8th Dist.). The City's argument turns this proposition on its head. The situation

[2] *See e.g., Grogan v. McGrath Rentcorp.*, No. 3:22-cv-00490 (N.D. Cal.); *Healy et al. v. Reiter Affiliated Companies, LLC*, Case No. 22-CV-003056 (Monterey County, Cal. Sup. Ct.); *Lucero v. Valex Corp.*, Case No. 56-2022-00570847-CU-NP-VTA (Ventura County, Cal. Sup. Ct.); *Yuan v. Hometrust Mortgage Co.*, No. 1 :22-cv-1355 (W.D. Tex.); *Medoff v. Minka Lighting, LLC*, Case No. 2:22-cv-08885 (C.D. Cal.).

in the present case is the reverse of the City's argument. Maintaining an IT System is routinely (and customarily) performed by private entities without any connection to government activities. That the City may also have to perform such tasks does not transform the activity customarily performed by nongovernmental persons into a governmental function.

Further, maintaining an IT System is not listed as a "governmental function" under R.C. 2744.01(C)(2). The City notes that the list enumerated under R.C. 2744.01(C)(2) is a "non-exhaustive list." Yet nothing in the enumerated list suggests that maintaining an IT System is a governmental function. In another effort to shoehorn its argument under R.C. 2744.01(C)(2), the City states that the creation of an IT infrastructure is essential to "nearly all" of the functions enumerated under R.C. 2744.01(C)(2). Mot. at 9. The use of information technology in multiple government functions does not transform that into a government function.

The case law relied upon by the City does not cure the fallacy of its argument. In *Doe v. Cleveland Metro. School Dist.*, 2012-Ohio-2497, ¶ 34 (8th Dist.), the court noted that "the act of distributing grants for educational purposes and assisting and overseeing the program for which those funds were provided are those customarily engaged in by governmental persons." Such activities, of course, are distinguishable from maintaining an IT System which is customarily engaged in by nongovernmental persons.

The City also relies on *Moncrief v. Bohn*, 2014-Ohio-837, ¶ 13 (8th Dist.), in which the court held that providing security at public housing was part of operating public housing, which is an enumerated government function under R.C. 2744.01(C)(2). *Id.* Similarly, in *Wolanin v. Holmes*, 2007-Ohio-3410, ¶ 11 (8th Dist.), which the City cites, the operation of a tram at a zoo is part of operating a zoo, which is an enumerated government function under R.C. 2744.01(C)(2)(u)(iii). By contrast, maintaining an IT System is not linked to any *particular* government function.

The City also misconstrues *Union Twp.-Clermont Cty., C.I.C., Inc. v. Lamping*, 2015-Ohio-1092, ¶ 19 (12th Dist.). In that case, the court analyzed an equitable estoppel argument which could not be asserted against the state in the exercise of a government function. *Id.* ¶ 18. The court held that the county building department had authority to make rules, which would include

providing information regarding those rules on a website, and incorrect information on the website could not be the basis for an equitable estoppel claim. *Id.* ¶¶ 19–21. The operation of a website as part of a specific government function is not analogous to the City maintaining an IT System. None of the cases cited by the City (nor any of its arguments) justifies designating maintaining an IT System as a "government function" for purposes of political subdivision immunity.

2. Maintaining an IT system with PII and confidential information is a proprietary function.

The City also argues that maintaining an IT System is not a "proprietary function," but in doing so, the City confusingly quotes only part of the relevant statutory definition. A "'Proprietary function' means a function of a political subdivision that is specified in [R.C. 2744.01(G)(2)] ***or*** that satisfies both of the following: (a) The function is not one described in [R.C. 2744.01(C)(1)(a) or (b)] and is not one specified in [R.C. 2744.01(C)(2)]; [and] (b) The function is one that promotes or preserves the public peace, health, safety, or welfare and that involves activities that are customarily engaged in by nongovernmental persons." R.C. 2744.01(G) (emphasis added).

Plaintiffs do not allege that maintaining an IT System with PII and confidential information falls under R.C. 2744.01(G)(2), so the City's argument in this regard is irrelevant. Further, as noted above, maintaining an IT System with PII and confidential information is not a function described under R.C. 2744.01(C)(a) or (b) and it is not specified under R.C. 2744.01(C)(2).

As Plaintiffs have alleged, maintaining an IT System 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. CAC at ¶¶ 18-19. Plaintiffs have adequately alleged that maintaining an IT System is a proprietary function. Moreover, Plaintiffs' allegations show "injury[] or loss to person or property caused by the negligent performance of acts by [the City's] employees with respect to proprietary functions of [the City]." *See* R.C. 2744.02(B)(2). Therefore, Plaintiffs have established that an exception applies under the second tier of the immunity analysis.

B. There are no applicable defenses under R.C. 2744.03(A) to restore the City's immunity.

The City lastly argues that, notwithstanding an exception to political-subdivision immunity, it has a defense under R.C. 2744.03(A)(5), which provides that "[t]he political subdivision is immune from liability if the injury, death, or loss to person or property resulted from the exercise of judgment or discretion in determining whether to acquire, or how to use, equipment, supplies, materials, personnel, facilities, and other resources unless the judgment or discretion was exercised with malicious purpose, in bad faith, or in a wanton or reckless manner." *Id.*

The City claims that the "maintenance of the City's IT infrastructure is unquestionably an exercise of judgment or discretion." Mot. at 11. The City's argument asks this Court to read the defense under R.C. 2744.03(A)(5) in an overly broad manner. Indeed, contrary to the City's argument, "courts must construe the R.C. 2744.03(A)(5) discretionary defense narrowly." *Leasure v. Adena Local School Dist.*, 2012-Ohio-3071, 973 N.E.2d 810, 818 (4th Dist.), citing *Greene Cty. Agricultural Soc. v. Liming*, 89 Ohio St.3d 551, 561 (2000).

As the Tenth District has held, R.C. 2744.03(A)(5) "protects only those charged with weighing alternatives and making choices with respect to public policy and planning characterized by a high degree of discretion and judgment. It does not protect a [political subdivision] from the negligent conduct of its employees in the details of carrying out the activity even though there is discretion in making choices. This is not the type of discretion for which there is immunity as it does not involve public policy endangering the creative exercise of political judgment." *Bolding v. Dublin Local School Dist.*, 1995 Ohio App. LEXIS 2455, *9 (10th Dist. June 15, 1995); *see also Inland Prods. v. City of Columbus*, 2011-Ohio-2046, ¶ 62 (10th Dist.) (noting that, under R.C. 2744.03(A)(5), "[i]mmunity attaches only to the broad type of discretion involving public policy made with 'the creative exercise of political judgment."), quoting *McVey v. Cincinnati*, 109 Ohio App.3d 159, 163 (1st Dist. 1995) and *Bolding*, 1995 Ohio App. LEXIS 2455, *9. "There is a difference between a political subdivision's discretionary decisions, for which there is immunity, and the employee[] implementation of those decisions, for which there is not." *Ohio Bell Tel. Co.*

v. City of Cleveland, 2024-Ohio-1475, ¶ 22 (8th Dist.). Thus, contrary to the City's argument, the defense under R.C. 2744.03(A)(5) does not involve the routine "discretionary" choices that would be involved in maintaining the City's IT infrastructure. Moreover, Plaintiffs are not alleging that the City's policy choice regarding protecting PII that would involve creative exercise of political judgment is the proximate cause of their injuries.

Even if the City could show that the defense under R.C. 2744.03(A)(5) applies, Plaintiffs have sufficiently alleged reckless conduct by the City to overcome the defense. "[R]eckless conduct is characterized by the conscious disregard of or indifference to a known or obvious risk of harm to another that is unreasonable under the circumstances and is substantially greater than negligent conduct." *Anderson v. City of Westlake*, 2021-Ohio-4582, ¶ 28 (9th Dist.). Here, given the extent of the breach at issue, which included release of PII of an undercover police officer, the only reasonable inference from Plaintiffs' allegations is that the City's conduct was characterized by a conscious disregard of or indifference to a known or obvious risk of harm to another that was unreasonable under the circumstances and was substantially greater than negligent conduct. CAC at ¶¶ 139, 149, 155.

Thus, Plaintiffs have alleged an exception to the City's political subdivision immunity under R.C. 2744.02(B)(2), and the City cannot establish a defense to the exception under R.C. 2744.03(A)(5).

II. Plaintiffs have standing.

The City complains that Plaintiffs lack standing because (1) the Complaint does not establish injury and (2) the alleged harms are not fairly traceable to the City's conduct. Mot. at 13–16. The City is wrong on both accounts.

To establish standing, Plaintiffs must show that they have suffered "(1) an injury that is (2) fairly traceable to the defendant's allegedly unlawful conduct, and (3) likely to be redressed by the requested relief." *Moore v. Middletown*, 133 Ohio St.3d 55, 2012-Ohio-3897, ¶ 22. Importantly, "[s]tanding does not depend on the merits of Plaintiffs' claims." *ProgressOhio.org, Inc. v.*

JobsOhio, 139 Ohio St.3d 520, 2014-Ohio-2382, ¶ 7. Standing depends, instead, on "whether the plaintiffs have alleged such a personal stake in the outcome of the controversy that they are entitled to have a court hear their case." *Id.* Plaintiffs have done so here.

A. Plaintiffs' allegations establish legally cognizable injuries.

1. Plaintiffs' injuries are actual and concrete.

Plaintiffs suffered at least five legally cognizable injuries due to the City's misconduct: (1) a privacy injury arising from the unauthorized disclosure of their PII, (2) damages to and diminution in the value of their PII, (3) imminent and impending injury arising from the substantially increased risk of identity theft, (4) lost time, annoyance, interference, and inconvenience in attempting to mitigate their injuries, and (5) anxiety, fear, stress, and increased concern for the loss of their privacy. CAC at ¶¶ 87–91. These injuries are actual and concrete and are sufficient to confer standing.

To establish standing, a party merely has to "alleg[e] enough general facts to show that injury resulted from the defendant's conduct." *S. Christian Leadership Conf. v. Combined Health Dist.*, 2010-Ohio-6550, ¶ 17 (4th Dist.). The injury "is not required to be large or economic"; it must only be "palpable." *League of United Latin Am. Citizens v. Kasich*, 2012-Ohio-947, ¶ 21 (10th Dist.). This concept is no different in the data breach context. After all, "it is difficult to conceive how the dissemination of an individual's PII does not necessarily diminish their control over their digital and physical identity. Such an invasion implicates non-economic harms." *Smallman* v. *MGM Resorts Int'l*, 2022 U.S. Dist. LEXIS 199399, *12 (D. Nev. Nov. 2, 2022). Privacy-related injuries are likewise recognized under Ohio common law. *See Motorists Mut. Ins. Co. v. Dandy-Jim, Inc*., 2009-Ohio-2270, ¶ 14 (8th Dist.) ("Ohio recognizes that the right of privacy includes both the right of seclusion and the right of secrecy.").

Importantly, the Sixth Circuit has expressly found that the injuries Plaintiffs allege here are enough to confer standing. *See Allen v. Wenco Mgmt., LLC*, 696 F. Supp. 3d 432, 437–38 (N.D. Ohio 2023) ("[T]he court is confident that Allen's alleged increased risk of identity theft gives him

standing to sue . . . given the connection between standing and damages, it also suggests the Supreme Court of Ohio would hold that such an injury is cognizable in negligence."); *Galaria v. Nationwide Mut. Ins. Co*., 663 F. App'x 384, 388 (6th Cir. 2016). And many courts around the country agree. *See Collins v. Athens Orthopedic Clinic, P.A.,* 307 Ga. 555, 562–64 (2019) (finding similar allegations "raise[d] more than a mere specter of harm" to survive a motion to dismiss); *Reetz v. Advocate Aurora Health, Inc*., 405 Wis.2d 298, 312–18 (Ct. App. 2022) (rejecting arguments that data breach plaintiff "failed to allege actual damages" and that "economic loss doctrine bars the claim," because "a data breach of PII creates a risk of future identity theft); *Bohnak v. Marsh & McLennan Companies, Inc*., 79 F.4th 276, 286 (2d Cir. 2023) (finding allegation that plaintiff had been "harmed by the exposure of her private information—including her SSN and other PII—to an unauthorized malevolent actor" fell "squarely within the scope of an intangible harm the Supreme Court has recognized as 'concrete'").

The City notably cites to a District of Maryland case from 2016 to suggest that "courts routinely" find allegations of a threat of future harm, including expenses to mitigate such harms, as too speculative to confer standing. Mot. at 13–14. Yet courts in the Sixth Circuit have repeatedly[3] held that the substantial risk of harm caused by a third-party data breach, coupled with reasonably incurred mitigation costs, is sufficient to establish Article III injury at the pleading stage. *See Galaria,* 663 F. App'x at 388. In *Galaria,* like here, Plaintiffs alleged that their data had been stolen and was now "in the hands of ill-intentioned criminals." *Id*. In finding a cognizable injury, the Sixth Circuit explained, "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints." *Id.* In such cases, "there is no need for speculation."

[3] *See also Brickman v. Maximus, Inc*., 2022 U.S. Dist. LEXIS 205627 (S.D. Ohio May 2, 2022) (following *Galaria* and finding standing in data breach case); *Haney v. Charter Foods N., LLC*, 2024 U.S. Dist. LEXIS 159245 (E.D. Tenn. Aug. 28, 2024) (same); *Lochridge v. Quality Temporary Servs*., 2023 U.S. Dist. LEXIS 113794 (E.D. Mich. June 30, 2023) (same); *Bowen v. Paxton Media Group, LLC*, 2022 U.S. Dist. LEXIS 162083 (W.D. Ky. Sep. 8, 2022).

Id. Although it might not be "literally certain" that Plaintiffs' data will be misused, there is a "sufficiently substantial risk of harm that incurring mitigation costs is reasonable." *Id*. Indeed, "[i]t would be unreasonable to expect Plaintiffs to wait for actual misuse." *Id.*

Plaintiffs have alleged—in no uncertain terms—that their data has been stolen and is currently in the hands of ill-intentioned criminals. CAC at ¶ 39. This is not speculative. Indeed, Plaintiffs provided screenshots of the criminal's auction of the stolen information. *Id*. at ¶¶ 39–41. In this case, like *Galaria*, criminals stole Plaintiffs' PII and are now selling it on the Dark Web. *Id*. The hackers targeted this data precisely because of its utility for identity theft. *Id*. at ¶¶ 94–100 (describing criminals' use of comprehensive dossiers called "Fullz" packages to sell PII). By offering employees and non-employees a year of credit monitoring (*id*. at ¶ 38), the City itself has tacitly recognized the severity of the risk. *See Galaria*, 663 F. App'x at 388 ("Nationwide seems to recognize the severity of the risk, given its offer to provide credit-monitoring and identity-theft protection for a full year."). Now, Plaintiffs face a risk of identity theft that is substantial and will continue for years. *Id.* at ¶¶ 87–91.

Moreover, many of the Plaintiffs have *already* suffered harm. John Does #1, #2, and #5's banking accounts were compromised shortly after the breach. *Id*. at ¶¶ 63, 70, 74. John Doe #3 has spent hours mitigating his risk. *Id*. at ¶ 72. And John Does #2 and #4 have since received threatening ransom notes. *Id*. at ¶¶ 71, 73. These injuries are not only monetary in nature; they are also emotionally taxing. John Doe #1, for example, is an undercover cop who fears that his identity will be exposed to people wishing him harm. *Id*. at ¶ 66. He now sleeps with a gun under his bed and has installed security cameras in his house. *Id*. at ¶ 69. The data breach exposed Plaintiffs' PII to criminals, thus impinging on their right to privacy and causing serious distress and anxiety. *See, e.g., id*. at ¶ 85 ("Jane Does fears for her personal financial security."). The breach has subjected Plaintiffs to a serious risk of identity theft, blackmail, and catastrophic financial losses. All this weighs heavily on Plaintiffs' mind, as the risk will be hanging over their heads for years to come. *Id*. at ¶ 91. Ohio law provides a remedy for these injuries.

2. Plaintiffs' allegations are specific enough to confer standing.

The City also faults Plaintiffs for not being specific enough regarding the information that has been stolen. Mot. at 13–14. But the City misconstrues Plaintiffs' obligations at this stage of litigation. Ohio is a notice pleadings state. *See Wells Fargo Bank, N.A. v. Wells*, 142 Ohio St.3d 416, 2015-Ohio-1484, ¶ 13 ("The purpose of 'notice' pleading is clear: 'to simplify pleadings to a 'short and plain statement of the claim' and to simplify statements of the relief demanded, Civ.R. 8(A), to the end that the adverse party will receive fair notice of the claim and an opportunity to prepare his response thereto.'") (citations omitted). "A plaintiff at the pleadings stage is not required to establish its standing beyond the allegations of the Complaint." *Id*. (citations omitted). Instead, at the pleading stage, the Court assumes the general allegations embrace the specific facts necessary to support the claim. *Bourke v. Carnahan*, 2005-Ohio-5422, ¶ 10 (10th Dist.). The City's argument that Plaintiffs must categorically list every type of PII that the City maintains on its servers directly contravenes Ohio's notice pleadings requirements.

Plaintiffs have alleged that the City "stores a litany of highly sensitive personally 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." (CAC at ¶ 3; *see also id.* at ¶¶ 24–27, 58, 78–79. In particular, John Does #1–5 are current employees who allege that the City received and maintained their PII as a condition of their employment. *Id.* at ¶¶ 8–12, 24. Jane Doe, in turn, is a non-employee citizen who alleges that the City received and maintained her PII when she entered City Hall in 2015 and when she paid a parking ticket. *Id.* at ¶¶ 78–79. Plaintiffs all allege that the City failed to reasonably secure their PII. *Id.* at ¶ 5. As a result, Plaintiffs have suffered and will imminently suffer injury. *Id.* at ¶¶ 87–91. These allegations are specific enough to provide fair notice of Plaintiffs' claims. The ultimate determination of whether Plaintiffs carried their burden to prove these allegations is a question for the jury to decide after a full record is developed.

B. Plaintiffs' injuries are fairly traceable to the City's conduct.

Finally, the City claims that Plaintiffs' injuries are not "fairly traceable" to the City's misconduct because it is "unclear who caused the supposed harm." Mot. at 15–16. But the "fairly traceable" element of standing "is not focused on whether the defendant 'caused' the plaintiff's injury in the liability sense," *Wuliger v. Mfrs. Life Ins. Co*., 567 F.3d 787, 796 (6th Cir. 2009), because "causation to support standing is not synonymous with causation sufficient to support a claim." *Parsons v. United States DOJ*, 801 F.3d 701, 715 (6th Cir. 2015). Ohio law only requires that plaintiffs sufficiently allege that their injuries are the natural and probable result of the defendant's conduct. *Bethel Oil & Gas, LLC v. Redbird Dev., LLC*, 2024-Ohio-5285, ¶ 67 (4th Dist.). "Consequently, 'the analysis of proximate cause and damages [is] 'not a matter of proof at the pleading stage; it is a matter for trial or, perhaps, for summary judgment if the facts are undisputed.'" *Id.*, quoting *Resor v. Dicke*, 2023-Ohio-4087, ¶ 28 (3d Dist.).

Here, Plaintiffs sufficiently allege that their injuries are fairly traceable to the City's conduct. As detailed above, Plaintiffs unequivocally allege that the City collected and maintained their PII and that the City's systems were breached by criminals. CAC at ¶ 101. Plaintiffs further allege that the City's failure to secure the sensitive personal information entrusted to it allowed the hackers to access Plaintiffs' PII. *Id*. at ¶¶ 1, 3, 49–51, 119, 123. John Does #1, #2, #4, and #5 and Jane Does all discovered that their data was on the Dark Web within weeks after the breach. *Id.* at ¶¶ 63, 70, 72–74, 81. And John Doe #3 immediately spent time attempting to mitigate his risk after learning about the breach. *Id*. at ¶ 72. Thus, Plaintiffs have sufficiently alleged that their injuries are the natural and probable result of the City's misconduct. *See Finesse Express, LLC v. Total Quality Logistics, LLC*, 2021 U.S. Dist. LEXIS 60648, *13 (S.D. Ohio Mar. 30, 2021) ("While Defendant is free to litigate at a later stage of the litigation whether the data breach caused Plaintiffs' fraudulent transactions, 'this debate has no bearing on standing to sue.'").

III. Plaintiffs' claims for negligence and negligence per se are well-pleaded.

The City moves to dismiss Plaintiffs' negligence claim, arguing that they failed to allege a duty, breach, or damages. Mot. at 16–21. To the contrary, there is ample authority demonstrating

that those who collect sensitive, personal information owe common law and statutory duties to safeguard that information from the foreseeable risk of a data breach. The detailed allegations of the 39 page complaint are plenty sufficient to establish a breach. And Ohio law unquestionably provides a remedy for those whose sensitive, personal information was exposed in a data breach. Therefore, the Court should deny the City's motion to dismiss.

A. Plaintiffs sufficiently alleged the existence of a duty.

The City argues that Plaintiffs have not alleged a common law or statutory duty. Mot. at 7–9. This argument fails on both points.

1. The City owed a common law duty to reasonably safeguard Plaintiffs' PII.

The City affirmatively collected and stored Plaintiffs' sensitive, personal information, which created a foreseeable risk of a data breach. It therefore owed Plaintiffs a common law duty of reasonable care.

As a general rule, "[t]he existence of a duty depends upon the foreseeability of the injury, which is determined by examining whether 'a reasonably prudent person would have anticipated that an injury was likely to result from the performance or nonperformance of an act.'" *Farley v. Duke Constr.*, 2008-Ohio-6419, ¶ 32 (10th Dist.), quoting *Fed. Steel & Wire Corp. v. Ruhlin Constr. Co.*, 45 Ohio St.3d 171, 173 (1989); *accord Cromer v. Children's Hosp. Med. Ctr. of Akron*, 142 Ohio St.3d 257, 2015-Ohio-229, ¶ 24; *Sens v. Fitness Int'l LLC*, 2023-Ohio-1004, ¶ 21 (10th Dist.). So, when someone engages in affirmative conduct that creates a risk to others, he has a corresponding duty to take reasonable precautions against foreseeable harms. *Parker v. L.T.*, 2017-Ohio-7674, ¶ 20 (1st Dist.) ("[A]ctors engaging in conduct that creates a risk to others have a duty to exercise reasonable care to avoid causing physical harm.").

Under Ohio law, those who collect sensitive, personal information owe a common law duty to safeguard that information from the foreseeable risk of a data breach. *See Tate v. EyeMed Vision Care, LLC*, 2023 U.S. Dist. LEXIS 175840, *23 (S.D. Ohio Sep. 29, 2023) (denying motion to dismiss because plaintiffs "alleged that data breaches are foreseeable and therefore [defendant]

owed a duty to take reasonable steps to prevent such breaches and the injuries flowing from them"). This is because collecting and maintaining PII is affirmative conduct that creates a risk of a data breach, which foreseeably harms those whose information is exposed in the breach. *See id.*; *Allen v. Wenco Mgmt., LLC,* 696 F. Supp. 3d 432, 440 (N.D. Ohio 2023) (denying motion to dismiss under Ohio law because "[plaintiff] alleges that [defendant] undertook affirmative conduct—collecting his PII—and breached its concomitant duty to 'protect [him] against an unreasonable risk of harm to [him] arising out of' that conduct"); *see also Brooks v. Peoples Bank*, 732 F. Supp. 3d 765, 779 (S.D. Ohio 2024) (holding under Kentucky law that "Plaintiffs have adequately pleaded [defendant] had a common law duty to safeguard their PII" based on allegation that "the risk of a data breach was a foreseeable consequence of [defendant] failing to safeguard Plaintiffs' PII").

Here, the City affirmatively collected highly sensitive PII from Plaintiffs. CAC at ¶¶ 58, 77, 86. The City thus had a duty to take precautions against the foreseeable consequences of that choice. *See Tate*, 2023 U.S. Dist. LEXIS 175840, *23; *Allen*, 696 F. Supp. 3d at 440. And it was highly foreseeable that hackers would target the information stored in the City's systems, given that this information is highly valuable on the black market and that municipalities are well known as prominent targets for data breaches. *See* CAC at ¶¶ 94–95, 104–113; *Tate*, 2023 U.S. Dist. LEXIS 175840, *23 (finding foreseeability based on allegation "that healthcare data breaches tripled from 2018 to 2019 and that 41 million patient records were compromised by data breaches in 2019 alone"); *see also Purvis v. Aveanna Healthcare, LLC,* 563 F. Supp. 3d 1360, 1369 (N.D. Ga. 2021) (finding foreseeability under Georgia law because "Plaintiffs allege that the threat of cyberattacks and data breaches was widely and publicly known"). Therefore, the City owed a common law duty of reasonable care.

2. The City owed statutory duties to Plaintiffs under the FTC Act.

Plaintiffs have also sufficiently pleaded a statutory duty under the doctrine of negligence per se, which "dispenses with the plaintiffs' burden to establish the existence of a duty and the breach

of that duty." *Wallace v. Golden Comb, Inc.*, 2013-Ohio-5320, ¶ 30 (8th Dist.). The City argues for three reasons that Section 5 of the FTC Act, 15 U.S.C. § 45, does not support a claim for negligence per se. Mot. at 18–19. None of those arguments has merit.

First, the City says that political subdivisions are not subject to Section 5. But Plaintiffs John Doe #1–5 brought this case against the City for its failure to safeguard PII that it collected within the scope of their employer-employee relationship. CAC at ¶¶ 8–12, 58, 70–75, 86. Employers are subject to Section 5's data security standards, as "the FTC has pursued complaints against companies who failed to secure the data of their employees under Section 5 of the FTC Act." *Covington v. Gifted Nurses, LLC*, 2023 U.S. Dist. LEXIS 141859, *24 (N.D. Ga. July 19, 2023) (denying motion to dismiss negligence per se claim in data breach case). Moreover, even if this claim were brought against the City in its capacity as a local government, rather than as an employer, the Supreme Court has denied a motion to enjoin an FTC enforcement action brought against a local government entity, thus rejecting the notion that municipalities are categorically exempt from the requirements of Section 5. *FTC v. Phoebe Putney Health Sys.*, 568 U.S. 216, 224 (2013).

Second, the City argues that Section 5 cannot provide the basis for negligence per se because it lacks a private right of action. This argument is inconsistent with Ohio's longstanding framework for negligence *per se*. "Where a statute . . . does not expressly provide for civil liability," the Ohio Supreme Court has held that "the question of whether violation of the statute constitutes negligence per se depends on the enactment itself." *Mussivand* v. *David*, 45 Ohio St.3d 314, 320 (1989). If the enactment "command[s] or prohibit[s] the doing of a specific act and there is a violation of such enactment solely by one whose duty is to obey it, such violation constitutes negligence per se." *Id.*, quoting *Eisenmuth* v. *Moneyhon*, 161 Ohio St.3d 367, 374 (1954). If, on the other hand, the enactment is too "general or abstract," then the doctrine does not apply. *Id.*

This framework expressly contemplates the application of negligence *per se* to enactments with no private right of action—i.e., a statute that "does not expressly provide for civil liability." *Id.* In *Reynolds*, for example, the Supreme Court noted that the statute in question did "not create

a cause of action" and had "no penalty provision," but nonetheless held that a violation was negligence *per se*. *Reynolds* v. *State Div. of Parole & Comm. Servs.*, 14 Ohio St.3d 68, 69 & n.1 (1984) (noting that a "statute need not . . . contain a specific civil penalty provision before its violation can constitute negligence *per se*"). Indeed, the Ohio Supreme Court has routinely held that violations of statutes with no private right of action constitute negligence *per se*. *See, e.g.*, *id.* at 70 n.4 (noting that the court had previously "found that a violation of R.C. 5321.04 . . . constitutes negligence *per* se and is actionable even though such statute does not provide for tort recovery"); *Crawford* v. *Halkovics*, 1 Ohio St.3d 184, 187 (1982) (holding that evidence showed "Crawford did not otherwise signal her intention to stop or suddenly decrease her speed, and that Crawford was thus in violation of R.C. 4513.071 and 4511.39 and negligent *per se*"). Thus, a violation of Section 5 may form the basis of a negligence *per se* claim despite that the statute lacks a private right of action.

Third, the City argues that Section 5 does not set forth a specific standard of conduct. Under Ohio law, a statute is sufficiently specific to support a claim for negligence *per se* if it sets forth a "fixed and absolute" standard of conduct. *Mann* v. *Northgate Investors, LLC*, 138 Ohio St.3d 175, 2014-Ohio-455, ¶ 30, quoting *Sikora v. Wenzel*, 88 Ohio St.3d 493, 498 (2000). In *Sikora*, the Ohio Supreme Court held that this standard was satisfied by R.C. 5321.04(A)(2), which requires landlords to "do whatever is reasonably necessary" to ensure the cleanliness of their buildings, concluding that this "statutory requirement is stated with sufficient specificity to impose negligence per se." *Sikora*, 88 Ohio St.3d at 498. The Court subsequently reaffirmed in *Mann* that this "reasonably necessary" standard contained the requisite "degree of specificity." *Mann*, 2014-Ohio-455, ¶ 32.

In this case, Section 5 of the FTC Act provides that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful." 15 U.S.C. § 45(a)(1). The statutory prohibition against "unfair methods of competition" and "unfair or deceptive acts" is at least as specific as the "reasonably necessary" standard from *Sikora* and *Mann*. Moreover, even if Section 5 were somewhat general on its face,

the FTC has extensively interpreted the text of the FTC Act and thereby "codified certain norms and best practices and has developed some baseline privacy protections. Standards have become so specific they resemble rules." Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 586 (2014). This "rather detailed list of inadequate security practices" provides an ascertainable standard of care. *Id.* at 650 (providing multi-page list of specific data security failures that the FTC has found to violate Section 5). *See* CAC at ¶¶ 114–119 (alleging violations of standard of care articulated by FTC).

Thus, "Section 5 of the FTCA is not too amorphous and vague to establish a fixed standard of care," particularly in light of the FTC's clear position regarding cybersecurity. *Perry v. Bay & Bay Transp. Servs.*, 650 F. Supp. 3d 743, 754 (D. Minn. 2023). Therefore, the City's alleged violations of Section 5 give rise to a duty enforceable through negligence per se. *See In re Marriott Int'l, Inc. Cust. Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 481 (D. Md. 2020) ("Section 5 of the FTC Act *is* a statute that creates enforceable duties. Moreover, this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data breach context."); *In re Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020) (same); *Purvis*, 563 F. Supp. 3d at 1373–74 (same).

B. Plaintiffs sufficiently alleged breach.

The City next asserts that Plaintiffs did not adequately plead a breach, arguing that Plaintiffs provided insufficient factual details regarding how its data security practices were deficient. Mot. at 19–20. This argument misapplies the pleading standard and ignores the allegations in the Complaint.

"Ohio is a notice pleading state," meaning that a complaint need only provide "fair notice" of the alleged misconduct. *Byrd v. Meyer*, 2022-Ohio-1827, ¶ 14 (10th Dist.). "This standard is different from the heightened federal plausibility standard of pleading, which has not been adopted by the Ohio Supreme Court. Thus, notice pleading does not require that the claim have 'facial

plausibility."' *S&T Bank, Inc. v. Advance Merchant Servs., LLC*, 2024-Ohio-4757, ¶ 55 (1st Dist.) (citations omitted); *see also State ex rel. Ware v. Booth*, 176 Ohio St.3d 349, 2024-Ohio-2102, ¶ 5 n.1 (confirming that Ohio "has never adopted" the "heightened federal pleading standard").

Here, Plaintiffs specifically alleged that the City breached numerous FTC standards and industry standards. CAC at ¶¶ 114–123. Plaintiffs further allege that the City maintained its data in a single, unified system for all City services and entities, which recklessly structured the City's data in such a way that a breach in any part of the City's system would give the hackers access to *all* of the City's data. *Id.* ¶¶ 2–3, 28, 50–51. The City may "disagree that the numerous standards and practices cited in" the complaint are applicable, but "the Court must accept Plaintiffs' allegations as true and draw all reasonable inferences in their favor." *Purvis*, 563 F. Supp. 3d at 1371 (denying motion to dismiss under Georgia law). Plaintiffs' allegations of breach are well-pleaded. *See Tate*, 2023 U.S. Dist. LEXIS 175840, *23 (holding that plaintiffs sufficiently alleged "that [defendant] breached that duty by failing to implement commonsense security protocols").

The City insists that Plaintiffs are required to provide an even more detailed factual analysis of its data security deficiencies. But as the City acknowledges, it has not cited a single case where an Ohio court demanded that level of specificity in the pleadings. Indeed, even under the heightened federal pleading standard, it is well-established that "data breach cases present unique challenges for plaintiffs at the pleading stage. A plaintiff may know only what the company has disclosed in its notice of a data breach. Even if some plaintiffs can find more information about a specific data breach, there are good reasons for a company to keep the details of its security procedures and vulnerabilities private from the public and other cybercriminal groups." *Ramirez v. Paradies Shops, LLC*, 69 F.4th 1213, 1220 (11th Cir. 2023). Thus, plaintiffs are not required "to plead with exacting detail every aspect of [the defendant's] security history and procedures that might make a data breach foreseeable[.]" *Id.*

The Eleventh Circuit's reasoning in *Ramirez* (which concerned duty) applies equally to the standard for pleading breach. "[V]irtually all of the details that [defendant] insists on" are within its exclusive possession, so "[i]t is unreasonable for [defendant] to insist that the details be laid out

in the initial complaint." *Flores-Mendez v. Zoosk, Inc.*, 2021 U.S. Dist. LEXIS 18799, *10–11 (N.D. Cal. Jan. 30, 2021); *accord Mehta v. Robinhood Fin. LLC*, 2021 U.S. Dist. LEXIS 253782, *18 (N.D. Cal. May 6, 2021) (applying *Flores-Mendez*). Given the asymmetrical access to information in data breach cases, by way of analogy, "*res ipsa loquitur* has some application here." *Flores-Mendez*, 2021 U.S. Dist. LEXIS 18799, *10–11. After all, the public generally expects that PII custodians "have taken adequate security steps to protect the security of that information from any and all hackers or interventions." *Id.* The public has "no clue," however, what these "security steps are," and there is "no way for users to know what security steps were actually in place." *Id.* Thus, "when a breach occurs, *the thing speaks for itself*. The breach would not have occurred but for inadequate security measures, or so it can be reasonably inferred at the pleadings stage." *Id.* Plaintiffs have sufficiently pleaded breach.

C. Plaintiffs sufficiently alleged legally cognizable injuries.

The City argues that Plaintiffs failed to allege damages. Mot. at 20–22. To the contrary, Plaintiffs suffered at least two legally cognizable injuries: (1) a privacy injury arising from the unauthorized disclosure of their PII in the data breach; and (2) the substantially increased risk of identity theft. Both are sufficient to support their negligence claims.

1. Plaintiffs suffered a privacy injury from the disclosure of their PII and PHI.

Plaintiffs suffered a legally cognizable privacy injury from the disclosure of their PII in the data breach. In *Allen*, the court held that a privacy injury caused by the disclosure of sensitive information in a data breach—there, the plaintiff's social security number—was sufficient to support a negligence claim. *Allen*, 696 F. Supp. 3d at 436–37. The court reasoned that the plaintiff's privacy injury was sufficient to support standing under Article III, which is an issue "closely related to damages." *Id.* And because the plaintiff had suffered an injury-in-fact for purposes of Article III, "that means that such an injury 'could support a claim for damages'" as well. *Id.*, quoting *Bohnak v. Marsh & McLennan Cos.*, 79 F.4th 276, 289–90 (2d Cir. 2023). *See also Doe v. Mission Essential Grp., LLC*, 2024 U.S. Dist. LEXIS 148732, *21 (S.D. Ohio Aug.

20, 2024) ("Plaintiff is correct that 'a plaintiff whose Social Security number is stolen in a data breach suffers concrete injury for the purpose of Article III standing.'"). Here, as discussed above, Plaintiffs suffered injuries sufficient to confer standing under Ohio law. *See supra* Part II. Those injuries are also sufficient to support a claim for damages.

The *Allen* Court's conclusion that a privacy injury is legally cognizable finds ample support in Ohio caselaw. *See Vinci v. American Can Co.*, 9 Ohio St.3d 98, 101 (1984) ("the injury, *i.e.*, the alleged invasion of privacy, is a common thread connecting all members of the class"). Courts have long recognized that a privacy injury may form the basis of a negligence claim. *See Prince v. St. Francis-St. George Hospital, Inc.*, 20 Ohio App.3d 4, 7 (1st Dist. 1985) ("[A] negligent invasion of the right of privacy . . . can just as effectively invade one's right of privacy as an intention to do so."); *Hanus v. McNeely*, 1993 Ohio App. LEXIS 5823, *7–8 (5th Dist.) (applying *Prince*); *Herman v. Kratche*, 2006-Ohio-5938, ¶ 41 (8th Dist.) ("Ohio recognizes the tort of negligent invasion of the right of privacy."); *Sowards v. Norbar, Inc.*, 78 Ohio App.3d 545, 555 (10th Dist. 1992) ("[A]n invasion of privacy need not be committed intentionally or maliciously in order to be actionable; simple negligence will suffice.").

The information exposed by the data breach in this case was highly sensitive, such that its exposure triggered a privacy injury. Plaintiff John Doe #1 is an undercover police officer with a well-founded fear that the exposure of his identity has placed his life in danger, particularly in light of his involvement in the seizure of tens of millions of dollars of narcotics from organized criminals. CAC at ¶¶ 57–60, 65–69. Indeed, the Sixth Circuit has held that similar information is entitled to protection under the constitutional right to privacy. *See Kallstrom v. City of Columbus*, 136 F.3d 1055, 1069 (6th Cir. 1998) (holding that undercover police officers had a constitutionally protected privacy interest in the confidentiality of their personally identifiable information). Likewise, Plaintiff John Doe #5 and Plaintiff Jane Doe had their social security numbers and other PII exposed in the breach (CAC at ¶¶ 74–84), which is the type of information that the Ohio Supreme Court has held is protected from disclosure under the constitutional right to privacy. *See State ex rel. Beacon Journal Publ'g Co. v. City of Akron*, 70 Ohio St.3d 605, 609–11 (1994)

(holding that the Ohio Constitution prohibited disclosure of social security numbers in response to public records request because "city employees have a legitimate expectation of privacy in their SSNs," and the theft of one's SSN enables identity theft, "perhaps the ultimate invasion of one's privacy"); *see also Krupa v. TIC Int'l Corp.*, 2023 U.S. Dist. LEXIS 4039, *4–5 (S.D. Ind. Jan. 10, 2023) (holding that plaintiff suffered injury sufficient to support negligence claim under Indiana law because "[t]here is a common-sense expectation . . . that social security numbers are best kept private and that their exposure to hackers is a harm (whether or not identity theft has yet occurred)"). The remaining Plaintiffs had sensitive PII such as financial information exposed in the breach (CAC at ¶¶ 70–73), which similarly is a sufficient injury to support a negligence claim. *See, e.g.*, *Mehta*, 2021 U.S. Dist. LEXIS 253782, *19 (holding that "Plaintiffs adequately allege[d] damages" based on "loss of control over the use of their identity" and "harm to their privacy" from disclosure of financial information); *Flores-Mendez*, 2021 U.S. Dist. LEXIS 18799, *11 (holding that "plaintiffs adequately allege[d] damages," including from the "loss of privacy with respect to highly sensitive information," such as emails and financial information). Therefore, Plaintiffs have suffered legally cognizable privacy injuries.

2. Plaintiffs suffered from an ongoing, increased risk of identity theft.

As a result of the data breach, Plaintiffs now face an increased risk of identity theft. That injury is cognizable under Ohio law.

In *Allen*, the court held that an "increased risk of identity theft is cognizable" and sufficient to support a negligence claim under Ohio law. *Allen*, 696 F. Supp. 3d at 438. That conclusion finds ample support in Ohio law. For example, the Ohio Supreme Court has recognized that an increased risk of harm is an injury sufficient to recovery in tort, most prominently in a medical monitoring case. *See Wilson v. Brush Wellman, Inc.*, 103 Ohio St.3d 538, 2004-Ohio-5847, ¶ 11–21; *Hirsch v. CSX Transp., Inc.*, 656 F.3d 359, 361 (6th Cir. 2011) (citing *Wilson* and noting "that court-supervised medical monitoring [is] available as an equitable remedy under Ohio law"). Medical monitoring is "a form of damages for an underlying tort claim." *Elmer v. S.H. Bell Co.*, 127 F.

Supp. 3d 812, 825 (N.D. Ohio 2015). Unlike other forms of tort damages, however, "[a] plaintiff need not demonstrate physical injuries" to obtain relief. *Id.* The rationale of these cases is that when a group is exposed to a potential toxin, "[s]ome individuals may never show symptoms or develop any disease, while others can have serious impairments or even die as a result of their exposure." *Wilson*, 817 N.E.2d at 61. Nonetheless, all of the victims will need to expend time, energy, and money monitoring their condition over the years. *See id.* at 63–65. Thus, an "increased risk" of harm opens the door to recovery in tort. *Elmer*, 127 F. Supp. 3d at 825 (quoting *Day v. NLO, Inc.*, 851 F. Supp. 869, 880 (S.D. Ohio 1994)).

This doctrine is equally applicable to the data breach context. *See Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633, 650 (N.D. Cal. 2020) (citing cases in which courts "have extended the toxic tort exception to data breach cases in which PII is compromised"); Daniel J. Solove & Danielle K. Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 772 (2018) (explaining why the heightened risk of identity theft following a data breach "is the digital equivalent to contracting a chronic disease"). Indeed, the Ohio Supreme Court has acknowledged the very risks that make a risk of identity theft analogous to a risk of a chronic disease. *See Beacon Journal*, 70 Ohio St.3d at 609–11. "Armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or social security benefits, order new checks at a new address on that person's checking account; obtain credit cards, or even obtain the person's pay check. Succinctly stated, the harm that can be inflicted from the disclosure of an SSN to an unscrupulous individual is alarming and potentially financially ruinous." *Id.* at 610 (cleaned up). The Court's recognition of the danger of improperly disclosing social security numbers signals that it would not hesitate to allow recovery for an increased risk of identity theft.

Moreover, as the *Allen* Court noted, this conclusion tracks federal Article III standing jurisprudence. *Allen*, 696 F. Supp. 3d at 438, citing *Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016). "The law from other jurisdiction largely supports" this conclusion, too. *Id.* In *Collins v. Athens Orthopedic Clinic*, for example, the Georgia Supreme Court held that "an imminent and substantial" risk of identity theft caused by a data breach is a legally cognizable

injury, regardless of whether any actual identity theft ever occurs. *Collins v. Athens Orthopedic Clinic*, 307 Ga. 555, 562–64 (2019); *see Purvis*, 563 F. Supp. 3d at 1371–72 (noting that none of the plaintiffs in *Collins* "had suffered *actual* identity theft"). And *Collins* is not an outlier. *See, e.g., Reetz v. Advocate Aurora Health, Inc.*, 405 Wis.2d 298, 312–18 (Ct. App. 2022) (rejecting arguments that data breach plaintiff "failed to allege actual damages" and that "economic loss doctrine bars the claim," because "a data breach of PII creates a risk of future identity theft"); *Huynh*, 508 F. Supp. 3d at 650 (applying medical monitoring caselaw to data breach under California law); *Sackin v. Transperfect Glob., Inc.*, 278 F. Supp. 3d 739, 749 (S.D.N.Y. 2017) (holding that plaintiff satisfied "the injury requirements of negligence" under New York law due to "imminent threat of identity theft" and need to mitigate the threat).

In this case, the data breach exposed sensitive PII, including social security numbers and financial information. CAC at ¶¶ 57–85. That information is publicly available on a dark web forum frequented by identity thieves. *Id.* ¶¶ 39–40. Unsurprisingly several Plaintiffs have now received notifications of attempted misuse of their PII. *Id.* ¶¶ 63, 70–75. As a result, Plaintiffs will face an increased risk of identity theft for many years to come. *Id.* ¶¶ 93–103. More importantly, Plaintiffs alleged in the Complaint that they suffered actual out-of-pocket damages to include paying for credit monitoring (*Id.* ¶ 72), ordering new checks (*Id.*), and installing a security system (*Id.* ¶ 69). Hence, there can be no legitimate argument that the occurrence of specific out-of-pocket expenses directly tied to the City's conduct coupled with the threat of the unauthorized use of Plaintiffs' PII are not cognizable injuries/damages under Ohio law.

D. The economic loss rule does not apply.

The City also claims that Plaintiffs' negligence claim is barred by the economic loss rule. Mot. at 20–21. But the economic loss rule does not apply here because (1) Plaintiffs have alleged non-economic personal injuries, and (2) their tort claims arise independent of any contractual duty.

1. Plaintiffs suffered non-economic personal injuries.

The economic loss rule does not apply because Plaintiffs suffered non-economic injuries. As a general matter, "three types of damages exist: (1) personal injury, (2) property damage, and (3) economic loss, which includes direct and indirect economic damages." *Breazeale v. Infrastructure & Dev. Eng'g, Inc.*, 2022-Ohio-4601, ¶ 7 (1st Dist.). The economic loss rule bars tort claims if the plaintiff seeks only the third type of damages—i.e., "purely economic loss." *Id.* at ¶ 6, quoting *Corporex Dev. & Constr. Mgt. v. Shook, Inc.*, 106 Ohio St.3d 412, 2005-Ohio-5409, ¶ 6. "[T]he law takes an expansive view of what counts as a personal injury. Defamation, for example, is regarded as inflicting a kind of personal injury: harm to the plaintiff's reputation." RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR ECONOMIC HARM § 2, cmt. a (2020).

Privacy injuries are similarly non-economic personal injuries. In *Allen*, for example, the court explained that under Ohio's economic loss rule, "[n]oneconomic loss includes any form of 'intangible loss.'" *Allen*, 696 F. Supp. 3d at 440, quoting *Whitaker v. M.T. Auto., Inc.*, 2006-Ohio-5481, ¶ 19. The plaintiff in that case alleged a privacy injury resulting from a data breach, and "[b]ecause such a loss is no doubt intangible—and thus noneconomic—the economic-loss rule doesn't apply." *Id.* Therefore, Plaintiffs' privacy injuries are non-economic. *See In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1142 (C.D. Cal. 2021) (rejecting economic loss rule argument under California law because "Plaintiffs have not alleged merely economic injury. Rather, they have alleged a privacy injury stemming from the unauthorized sharing of their private medical information."); *Smallman*, 2022 U.S. Dist. LEXIS 199399, *12 (holding that under Nevada law a privacy injury diminishes the plaintiff's "control over their digital and physical identity" and thus "implicates non-economic harms").

2. The City owed a duty independent of any contract, so the economic loss rule does not apply.

Even if Plaintiffs' injuries were purely economic, there is no contract between the parties that regulates data security. Consequently, the City's common law and statutory tort law duties are independent of any contractual agreement, so the economic loss rule does not apply.

Under the economic loss rule, "a party cannot recover in tort for purely economic loss for the breach of a duty that arose *solely* by contract." *Ineos USA LLC* v. *Furmanite Am., Inc.*, 2014-Ohio-4996, ¶ 19 (3d Dist.) (emphasis added). But if "a tort claim alleges a duty was breached independent of the contract, the economic loss rule does not apply." *Windsor Med. Ctr., Inc.* v. *Time Warner Cable, Inc.*, 2021-Ohio-158, ¶ 28 (5th Dist.). After all, the economic loss rule only "precludes common-law tort claims for financial loss based on negligent conduct *that the contract regulates*." *Allen*, 696 F. Supp. 3d at 440 (emphasis added), quoting RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR ECONOMIC HARM § 3, cmt. c (2020). This is because the rationale of the economic loss rule—that parties to a contract "should remain free to govern their own affairs" and limit their damages to those "which were within the contemplation of the parties when framing their agreement"—does not apply when a tort claim arises from conduct not regulated by the contract. *Corporex Dev. & Constr. Mgmt.* v. *Shook, Inc.*, 106 Ohio St.3d 412, 2005-Ohio-5409, ¶ 6, 10 ("When a duty in tort exists, a party may recover in tort. When a duty is premised entirely upon the terms of a contract, a party may recover based upon breach of contract.").

Here, Plaintiffs pleaded valid common law and statutory duties. *See supra* Part III.A. Those claims are not premised on the existence of any contractual agreement regulating data security. Indeed, the City has affirmatively argued that there is no such contractual agreement, which confirms that Plaintiffs' claims arise independent of any contractual duty. *See Allen*, 696 F. Supp. 3d at 440 (holding that the economic loss rule did not apply because there was "no contractual duty on [defendant's] part to regulate data security," meaning that "if [defendant] had *any* duty to protect [plaintiff's] PII, it must have been 'a discrete, preexisting duty in tort'"). Therefore, the Court should deny the City's motion to dismiss. *See In re Banner Health Data Breach Litig.*, 2017 U.S. Dist. LEXIS 221534, *28 (D. Ariz. Dec. 20, 2017) ("Plaintiffs have as of yet failed to allege adequately the existence of a contract governing data security between the parties, making it inappropriate to dismiss their claim for negligence at this stage in the litigation based on a rule designed solely for the purpose of distinguishing contractual and tort duties.").

IV. Plaintiffs sufficiently alleged a claim for breach of fiduciary duty.

Plaintiffs have also alleged a viable breach of fiduciary duty claim. A breach of fiduciary duty requires "(1) the existence of a duty arising from a fiduciary relationship; (2) a failure to observe the duty; and (3) an injury resulting proximately therefrom." *Akerstrom v. 635 W. Lakeside, Ltd.*, 2018-Ohio-98, ¶ 18 (8th Dist.). "[T]he determination of what constitutes a fiduciary relationship is a question of fact dependent on the circumstances of each case." *Gracetech Inc. v. Perez*, 2012-Ohio-700, ¶ 12 (8th Dist.). A fiduciary relationship may arise from a "confidential relationship, wherein 'one person comes to rely on and trust another in his important affairs and the relations there involved are not necessarily legal, but may be moral, social, domestic, or merely personal.'" *Hoffman v. Atlas Title Solutions, Ltd.*, 2023-Ohio-1706, ¶ 46 (3d Dist.).

Courts have recognized the mandatory receipt of sensitive, confidential information gives rise to a fiduciary relationship. *See Tucker v. Marietta Area Health Care, Inc.*, 2023 U.S. Dist. LEXIS 13974, *18 (S.D. Ohio Jan. 26, 2023) ("Ohio recognizes that medical providers, like MHS, hold 'a fiduciary position' with patients and have a duty to keep patient's medical information confidential."); *Herman v. Kratche*, 2006-Ohio-5938, ¶ 20 (8th Dist.) ("There is no dispute that the Clinic, as plaintiff's medical provider, held a fiduciary position with plaintiff as its patient and had a duty to keep plaintiff's medical information confidential."). Here, Plaintiffs have alleged that the City required Plaintiffs to provide it with PII and confidential information. Plaintiffs entrusted this information to the City, and the City in turn agreed to not to disclose such information to nefarious actors and cybercriminals. As Plaintiffs have alleged, the City breached this duty by failing to maintain the security of its IT System. Further, Plaintiffs have been damaged as a result of the City's breach of its fiduciary duty to Plaintiffs.

CONCLUSION

The Court should deny the City's motion to dismiss.

Respectfully submitted,

Date: February 13, 2025

By: /s/ *Jared W. Connors*

Matthew R. Wilson (72925)
Jared W. Connors (101451)
MEYER WILSON CO., LPA
305 W. Nationwide Blvd.
Columbus, OH 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066
mwilson@meyerwilson.com
jconnors@meyerwilson.com

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

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.co
zschiff@schifflegal.com

Counsel for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I certify that on February 13, 2025 the foregoing was filed using the Court's CM/ECF system and therefore will be electronically served to all parties' counsel of record.

/s/ *Jared W. Connors*
Jared W. Connors

Exhibit A

IN THE COURT OF COMMON PLEAS, FRANKLIN COUNTY, OHIO
CIVIL DIVISION

THE CITY OF COLUMBUS, Plaintiff, v. DAVID LEROY ROSS, JR. Defendant.	Case No. Judge

AFFIDAVIT OF ELAINE BRYANT

STATE OF OHIO,
COUNTY OF FRANKLIN, SS

Upon being duly sworn according to law, Affiant deposes and states as follows:

1. My name is Elaine Bryant. I am the Chief of Police for the City of Columbus.

2. I have knowledge of the facts set forth in this Affidavit. If called upon to testify as to the facts stated in this Affidavit, I could and would testify competently and truthfully thereto. I am over 18 years of age.

3. I am aware that the City of Columbus was the victim of a massive cyber-attack targeting some of the City's most sensitive databases containing individuals' personal information.

4. As part of my job duties as the Chief of Police I have been informed that David Leroy Ross, Jr. has accessed and downloaded the City's stolen date from the dark web and shared the stolen data with others.

5. I have also been informed that on the afternoon of August 28, 2024, the City was notified by several media contacts that Mr. Ross showed them records stolen by the foreign criminals which Mr. Ross claims to have pulled down from the dark web and that reveal the identities of undercover police officers, minor victims of crime, and more.

6. The irreparable harm that could be done by the readily-accessible public disclosure of this information locally by Mr. Ross is a real and ongoing threat.

7. Obtaining, using, and disclosing that confidential data with flagrant disregard for any increased risk of harm to which it could expose the City, our police officers (particularly our undercover officers), and their families, crime victims and their families, and witnesses and their families, harms the City.

Further, Affiant sayeth naught.

Elaine Bryant

State of Ohio)

County of Franklin) SS:

Before me, a Notary Public, personally appeared Elaine Bryant who under oath executed the foregoing instrument and acknowledged before me that he/she executed the same freely and voluntarily for the purposes therein expressed.

SWORN TO AND SUBSCRIBED before me this 29th day of August, 2024.

Notary Public

Printed Name: Maria J. Myers

My Commission Expires: March 6, 2029

Maria J. Myers
Notary Public, State of Ohio
My Commission Expires 03-06-2029

Exhibit B

IN THE COURT OF COMMON PLEAS, FRANKLIN COUNTY, OHIO
CIVIL DIVISION

THE CITY OF COLUMBUS, Plaintiff, v. DAVID LEROY ROSS, JR. Defendant.	Case No. Judge

AFFIDAVIT OF SAM ORTH

STATE OF OHIO,
COUNTY OF FRANKLIN, SS

Upon being duly sworn according to law, Affiant deposes and states as follows:

1. My name is Sam Orth. I am the Director of Technology for the City of Columbus.

2. I have knowledge of the facts set forth in this Affidavit. If called upon to testify as to the facts stated in this Affidavit, I could and would testify competently and truthfully thereto. I am over 18 years of age.

3. On July 18, 2024, the City of Columbus became aware it was the victim of a massive cyber attack.

4. The City soon thereafter confirmed that a foreign cyber criminal network, Rhysida, attempted to disrupt the City's IT infrastructure and stole copies of some of the City's most sensitive databases containing individuals' personal information.

5. The City's investigation of the cyber attack continues around the clock.

6. The City has determined that the foreign cyber criminals gained unauthorized access to the City's technology infrastructure, which included, but is not limited to, the criminals'

theft of highly sensitive personal data from the City Attorney's Office prosecutor backup database and the crime backup database.

7. On July 31, 2024, the foreign criminals advertised some portion of the City's stolen information for auction on the Internet's dark web, a place for criminals to go and use bitcoin to purchase stolen information they would use to do harm to others. On August 8, 2024, when the Rhysida auction failed, some of the City's stolen data was posted to the dark web.

8. Only individuals willing to themselves navigate and interact with the criminal element on the dark web, who also have the computer expertise and tools necessary to download data from the dark web, would be able to do so.

Further, Affiant sayeth naught.

Sam Orth

State of Ohio)

County of Franklin) SS:

Before me, a Notary Public, personally appeared Sam Orth who under oath executed the foregoing instrument and acknowledged before me that he/she executed the same freely and voluntarily for the purposes therein expressed.

SWORN TO AND SUBSCRIBED before me this 29th day of August, 2024.

Notary Public

Printed Name: Maria J. Myers

My Commission Expires: March 6, 2029

Maria J. Myers
Notary Public, State of Ohio
My Commission Expires 03-06-2029

Exhibit C

IN THE COURT OF COMMON PLEAS, FRANKLIN COUNTY, OHIO
CIVIL DIVISION

THE CITY OF COLUMBUS, Plaintiff, v. DAVID LEROY ROSS, JR. Defendant.	Case No. Judge

AFFIDAVIT OF LARA BAKER-MORRISH

STATE OF OHIO,
COUNTY OF FRANKLIN, SS

Upon being duly sworn according to law, Affiant deposes and states as follows:

1. My name is Lara Baker-Morrish. I am the Deputy City Attorney.

2. I have knowledge of the facts set forth in this Affidavit. If called upon to testify as to the facts stated in this Affidavit, I could and would testify competently and truthfully thereto. I am over 18 years of age.

3. Among the data stolen from the City and presumably posted to the dark web are two backup databases that contain large amounts of data gathered by City prosecutors and the Columbus Division of Police pertaining to misdemeanor crimes prosecuted by the City's Attorney's office dating back to at least 2015.

4. This data would potentially include sensitive personal information of police officers, as well as the reports submitted by arresting and undercover officers involved in the apprehension of the persons charged criminally by the City prosecutor's office.

5. These backup databases also contain the personal information of crime victims of all ages, including minors, and witnesses to the crimes the City prosecuted from at least 2015 to the present.

Further, Affiant sayeth naught.

Lara Baker-Morrish

State of Ohio)

County of Franklin) SS:

Before me, a Notary Public, personally appeared Lara Baker-Moorish who under oath executed the foregoing instrument and acknowledged before me that he/she executed the same freely and voluntarily for the purposes therein expressed.

SWORN TO AND SUBSCRIBED before me this 29th day of August, 2024.

Notary Public

Printed Name: Maria J. Myers

My Commission Expires: March 6, 2029

Maria J. Myers
Notary Public, State of Ohio
My Commission Expires 03-06-2029