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

THE CITY OF COLUMBUS, Plaintiff, v. DAVID LEROY ROSS, JR., Defendant.	Case Judge

MOTION FOR EX PARTE TEMPORARY RESTRAINING ORDER

Pursuant to Civ.R. 65(A), Plaintiff City of Columbus ("the City") respectfully moves this Court for a temporary restraining order enjoining Defendant David Leroy Ross, Jr. from accessing, and/or downloading, and/or disseminating the City's data that has been stolen as part of a massive cyber-attack of the City's IT system. The requested TRO should be granted without prior written or oral notice to the Defendant for the reasons stated in the attached attorney certification.

A memorandum supporting this motion is attached hereto.

Respectfully submitted,

/s/ Westley M. Phillips
Westley M. Phillips (0077728) – LEAD
Paul M. Bernhart (0079543)
Assistant City Attorneys
CITY OF COLUMBUS, DEPARTMENT OF LAW
ZACH KLEIN, CITY ATTORNEY
77 N. Front Street, Columbus, Ohio 43215
(614) 645-7385 / (614) 645-6949 (fax)
wmphillips@columbus.gov
pmbernhart@columbus.gov

Attorneys for Plaintiff City of Columbus

MEMORANDUM IN SUPPORT

I. FACTUAL BACKGROUND

On July 18, 2024, the City became aware it was the victim of a massive cyber-attack. ORTH AFF. ¶ 3 (attached as EX. A). 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. *Id*. at ¶ 4. The City's investigation of the cyber-attack continues around the clock. *Id*. at ¶ 5. 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 from the crime backup database. *Id*. at ¶ 6.

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. *Id*. at ¶ 7. On August 8, 2024, when the Rhysida auction failed in whole or in part, some of the City's stolen data was posted to the dark web. *Id*. Among the data stolen from the City and presumably posted to the dark web are the two backup prosecutor and crime databases. *Id* at ¶ 6. These databases contain large amounts of data gathered by the 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. BAKER-MORRISH AFF. ¶ 3 (attached as EX. B). 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 persons charged criminally by the City prosecutor's office. *Id*. at ¶ 4. These 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. *Id*. at ¶ 5.

On August 13, 2024, Andrew Ginther, Mayor of the City of Columbus, gave a series of interviews detailing the broad outline of the facts of the cyber-attack as well as the City's response to date. FENNING AFF. ¶ 4 (attached as EX. C). Later that same day, the City was contacted by a reporter from the Columbus NBC affiliate seeking comment for stories to run that evening alleging that Defendant had taken it upon himself to access and download the City's stolen data from the dark web. *Id*. at ¶ 5. Defendant shared the stolen data he had recovered with the media.[1] Media outlets used the stolen data provided by Defendant to go door-to-door and otherwise contact individuals whose names were on the stolen data.[2]

From August 13, 2024 to date, Defendant has provided numerous interviews to local media outlets and has used the City's stolen data to reveal the personal information of innocent individuals—visitors to City Hall, victims of domestic violence and other misdemeanor offenses, and lists of individuals allegedly compiled to prevent their access to City buildings, just to name a few.[3] Defendant's actions of downloading from the dark web and spreading and threatening to spread this stolen, sensitive information at a local level has resulted in widespread concern

[1] Meighan, S. (2024, August 13). Ginther defends city's response after cybersecurity expert says breach leaked citizen data. *Columbus Dispatch*; Levine, S. (2024, August 15). Crime victim caught up in Columbus data breach nightmare demands answers after info stolen. *CW Columbus*; Jabour, T. (2024, August 15). *Former FBI agent gives insight on Columbus cyberattack*. WBNS 10TV; Jabour, T. (2024, August 22). *Columbus Mayor Andrew Ginther confirms personal information on dark web following cyberattack*. WYSO; and Feuerborn, M. (2024, August 26). *Where Columbus stands after data leak: what you should know*. WCMH.

[2] Cleary, I., Beachy, K. & Feuerborn, M. (2024, August 14). *Confirmed: Columbus data leak affects residents, and what has been released*. Fox8 News.

[3] *Id*. See also Meighan, S. (2024, August 13). Ginther defends city's response after cybersecurity expert says breach leaked citizen data. *Columbus Dispatch*; Levine, S. (2024, August 15). *Crime victim caught up in Columbus data breach nightmare demands answers after info stolen*. CW Columbus; Jabour, T. (2024, August 15). *Former FBI agent gives insight on Columbus cyberattack*. WBNS 10TV; Jabour, T. (2024, August 22). *Columbus Mayor Andrew Ginther confirms personal information on dark web following cyberattack*. WYSO; and Feuerborn, M. (2024, August 26). *Where Columbus stands after data leak: what you should know*. WCMH.

throughout the Central Ohio region.[4] Only individuals willing to 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. ORTH AFF. ¶ 8. The dark web-posted data is not readily available to for public consumption. Defendant is making and threatening to make it so.

At various times throughout his interviews, Defendant has alluded to the existence of potentially even more troubling data having been exfiltrated by the foreign criminals, baiting the news reporters and public alike to continue to turn to him for more details as to the stolen data.[5]

On the afternoon of August 28, 2024, the City was notified by several media contacts that Defendant showed them records stolen by the foreign criminals which Defendant claims to have pulled down from the dark web and which he claims to reveal the identities of undercover police officers, minor victims of crimes and more. FENNING AFF. ¶ 6. The irreparable harm that could be done by the readily-accessible public disclosure of this information locally by Defendant is a real and ongoing threat. BRYANT AFF. ¶ 6 (attached as EX. D). Defendant is threatening to publicly disclose and disseminate the City's stolen data to the local community in the form of a website he will himself create.[6] This after Defendant went onto the dark web, downloaded the stolen data, and contacted media outlets to disclose that he has obtained and is threatening to share the City's stolen

[4] Levine, S. (2024, August 15). *Crime victim caught up in Columbus data breach nightmare demands answers after info stolen*. CW Columbus;

[5] Hoffman, B & Cleary, I. (2024, August 16*). Columbus extends free credit monitoring to anyone affected by data leak*. WCMH; Feuerborn, M. & Cleary, I. (2024, August 19). *'Gut-wrenching:' More victims found in Columbus data leak*. WCMH.

[6] Cleary, I. & Hofmann, B. (2024, August 15). *New records uncovered from Columbus data leak: protection orders, court records involving juveniles*. NBC4.

data with third parties who would otherwise have no readily available means by which to obtain the City's stolen data.

From at least August 13, 2024 to the present, Defendant has been contacting media, the entire time the criminal investigation by the City was ongoing, claiming to have access to and disclosing information stolen from the City by the criminal threat actors. Defendant downloading from the dark web and sharing publicly the City's stolen confidential data interferes with the City's ongoing criminal investigation into the cyber-attack. His threats to spin up his own website where the public can readily access this information threatens the City Attorney's prosecutions and could lead to the exposure of the identity of undercover officers. Improperly obtaining, using and disclosing the City's stolen confidential data with flagrant disregard for any increased risk of harm to which Defendant could be exposing the City, its police officers, (and, in particular, undercover police officers), and their families, crime victims and their families, and witnesses and their families harms the City. BRYANT AFF. ¶ 7.

II. LAW AND ARGUMENT

A. STANDARD FOR THE ISSUANCE OF A TEMPORARY RESTRAINING ORDER

A temporary restraining order is an equitable remedy needed to maintain the status quo until an orderly resolution of the issues can be achieved. It should be granted to prevent injustice, protect rights, and prevent injury where legal remedies will be inadequate. *Gobel v. Laing* (1967), 12 Ohio App.2d. 93. In determining the propriety of a motion for a temporary restraining order, Ohio courts generally consider and balance the following four factors:

(1) Whether the moving party has shown a likelihood or probability of success on the merits;

(2) Whether the moving party has shown immediate and irreparable injury that will result if the temporary restraining order is not issued;

(3) Whether the potential harm to others will occur; and

(4) Whether the public interest will be best served by issuing the injunction.

City of Cleveland v. Cleveland Electric Illumination Co. (1996), 115 Ohio App.3d 1, 684 N.E.2d 343; see also, *Garono v. State* (1988), 37 Ohio St. 3d 171, 173; R.C. 2727.02. In this case, each of these four factors has been conclusively satisfied and the City is entitled to the requested temporary restraining order.

B. THE CITY HAS A SUBSTANTIAL LIKELIHOOD OF SUCCESS ON THE MERITS

Defendant's own statements made during multiple media appearances proves that he accessed and downloaded the City's stolen data from the dark web and shared the stolen data with others. Media outlets showed Defendant displaying the stolen data to journalists. Members of the media then contacted the individuals whose names were found in the stolen data provided to the media by Defendant. The City has been notified by several media contacts that Defendant showed them the City's stolen data and that the Defendant purports that the data reveals the identities of undercover police officers, minor victims of crimes and more.

Defendant's conduct is in violation of multiple provisions of the Ohio Revised Code and Columbus City Codes. He has violated and continues to violate O.R.C. § 2923.04 by knowingly disseminating information gained from access to the law enforcement automated database and the Ohio law enforcement gateway. He has violated and continues to violate O.R.C. § 2913.51 by receiving stolen property. He has violated and continues to violate O.R.C. § 2921.04 by knowingly attempting to intimidate or hinder victims of crime in the prosecution of criminal charges and by intimidating witnesses to criminal acts. He has violated and continues to violate Columbus City Code § 2321.04 by knowingly attempting to intimidate or hinder victims of crime in the filing and prosecution of criminal charges and of witnesses in criminal cases in the discharge of their duty.

He has violated and continues to violate Columbus City Code § 2317.31 by committing the criminal offenses identified above and causing a serious public inconvenience and alarm. And regarding Defendant's violations of the Columbus City Codes, C.C.C. § 101.08 specifically states that "whenever there is a violation of any provision of the Columbus City Codes, the official charged with the responsibility to enforce said provision may immediately file a complaint for injunctive relief in the appropriate court of competent jurisdiction."

Defendant is also liable under multiple tort theories. He is liable for an invasion of privacy for wrongfully intruding into, downloading, and publicly disseminating the private and confidential information of the City, causing irreparable harm and damages to the City. He is liable for negligence because he has failed to act as a reasonably prudent person, causing irreparable harm and damages to the City. He is liable for civil conversion because he has wrongfully exercised dominion and control over the City's property and has wrongfully converted the same into his own use and benefit to the exclusion of and inconsistent with the City's ownership of its property.

For any and all of these reasons, the City has a substantial likelihood of success on the merits in this case.

C. THE CITY WILL SUFFER IMMEDIATE AND IRREPARABLE HARM

Defendant's continued conduct is dangerous and will result in irreparable harm to the City. He is interfering with the City's ongoing criminal investigation into the cyber-attack and the City Attorney's prosecutions. If he follows through with his stated intentions, he is going to disseminate stolen records that reveal the identities of undercover police officers, minor victims of crimes and more. The irreparable harm that could be done by Defendant making readily-accessible the public disclosure of the City's confidential information locally to those who might seek to use it to do harm is a real and ongoing threat to the City.

D. NO HARM TO OTHERS WILL OCCUR IF THE TRO IS GRANTED

While the City will suffer irreparable harm if the Defendant is not enjoined, Defendant will not be harmed at all by the granting of this temporary restraining order. He has no right to access, download, and disseminate the City's stolen data and he has no property interest in the City's stolen data.

E. A TEMPORARY RESTRAINING ORDER WILL PROTECT THE PUBLIC INTEREST

The public interest weighs very heavily in favor of issuing a temporary restraining order in this case. The TRO will not only protect the public interest, it will literally protect the safety of undercover police officers, minor victims of crimes, and more.

III. CONCLUSION

For the reasons stated above, a temporary restraining order is essential to maintain the status quo in order to prevent immediate and irreparable harm to the City. The City has no adequate remedy at law. Defendant David Leroy Ross, Jr. must be temporarily enjoined from accessing, and/or downloading, and/or disseminating the City's stolen data. Further, Defendant must be ordered to preserve and not to alter the data that he has downloaded to date.

Respectfully submitted,

/s/ Westley M. Phillips
Westley M. Phillips (0077728) – LEAD
Paul M. Bernhart (0079543)
Assistant City Attorneys
CITY OF COLUMBUS, DEPARTMENT OF LAW
ZACH KLEIN, CITY ATTORNEY
77 N. Front Street, Columbus, Ohio 43215
(614) 645-7385 / (614) 645-6949 (fax)
wmphillips@columbus.gov
pmbernhart@columbus.gov

Attorneys for Plaintiff City of Columbus

CERTIFICATE OF SERVICE

I hereby certify that, on **August 29, 2024**, I electronically filed the foregoing with the Court using the Court's CM/ECF system.

/s/ Westley M. Phillips
Westley M. Phillips (0077728)