



March 13, 2024

City Manager Batista

City of Worcester

*Delivered via email*

Dear Manager Batista:

On behalf of the ACLU of Massachusetts, Common Cause, Massachusetts Budget and Policy Center, MassPIRG, and the New England First Amendment Coalition, we write to raise serious concerns about your decision to end the City of Worcester's Open Checkbook program and ask you to reverse course and restore the program as soon as practicable.

Fiscal transparency is a hallmark of open government. Taxpayers, journalists, and civil society organizations must have access to information about government expenditures to ensure government is functioning appropriately, without corruption or mismanagement.

While cybersecurity is a serious issue and should be prioritized by government at every level, there is nothing about Open Checkbook data that poses a unique cybersecurity threat. In fact, the records accessible in Open Checkbook are public under state law and other municipalities and the state government continue to use their own portals. Concerns about hacking related to this data, like any other public data online, can be addressed by implementing and adhering to basic cybersecurity practices and policies. It is not possible to rid the world of threats, and in our collective response to them, we must consider and prioritize other values, such as democratic accountability, independent oversight, and transparency.

Under your leadership, the City of Worcester has identified "maintaining a sound fiscal government" as a top priority. Your administration has also pledged to be transparent. Yet absent access to Open

Checkbook data, it is very difficult for residents to assess how effectively the City is meeting its goals. Reversing course on a successful open government program that was in place for over a decade cuts against your stated commitment to transparency.

Public reporting about the decision to end the Worcester Open Checkbook program indicates that the decision was in part motivated by an incident that took place in Pennsylvania, where a water authority was hacked in retaliation for the ongoing violence in Gaza. However, the federal government determined that the Pennsylvania hack was the result of basic cybersecurity failures pertaining to passwords and network issues, not the consequence of any government transparency program.<sup>1</sup>

We appreciate your well-founded concern about cybersecurity threats to City government, particularly given the rise of artificial intelligence and the associated risks to critical infrastructure. But government secrecy about something as foundational as government expenditures is not the answer to these problems. Indeed, we are unable to identify a single cybersecurity authority that recommends such drastic action as ending open access to public financial information as a means of preempting hacking threats.<sup>2</sup>

This is Sunshine Week, a time when the journalism, civic, education, government and private sectors collaborate to shine a light on the importance of open government. It does not reflect well on Worcester, and it does a disservice to its residents, to plunge the city's finances into darkness. Cutting off access to basic information about how residents' tax dollars are spent is unwarranted and unwise, and we urge you to promptly restore public access to this vital information.

Sincerely,

ACLU of Massachusetts

Common Cause

Massachusetts Budget and Policy Center

MassPIRG

New England First Amendment Coalition

Cc: Worcester City Council

---

<sup>1</sup> Frank Bajak and Marc Levy, "Congressmen ask DOJ to investigate water utility hack, warning it could happen anywhere," November 30, 2023, Associated Press. <https://apnews.com/article/cybersecurity-water-wastewater-israel-hacker-iran-12fc7398a4ed6e6f7a47e83531c50c87>

<sup>2</sup> Indeed, Bloomberg Philanthropies' What Works Cities program specifically refutes the claim that open data programs could harm municipal cybersecurity: "There are no known examples of cybersecurity attacks where government data has been inappropriately obtained through open data portals." <https://labs.centerforgov.org/open-data/addressing-concerns/>