Formal Notice: Active Data Breach Involving Resident PII

1 message

Adam Whitaker <adam@wakepublishing.com> Thu, Jan 15, 2026 at 12:31 AM
To: laurie.hohe@apexnc.org, Randy Vosburg <randy.vosburg@apexnc.org>

Town Manager Vosburg and Town Attorney Hohe -

I am writing to you both in my capacity as the Publisher of The Peak Weekly to formally notify the Town of Apex of a critical data security vulnerability involving the personal information of over 500 residents.

During a review of Council Member Mahaffey's "2026 CIP Survey" application hosted on his personally-owned wakeresults.org server (and its associated GitHub repository terrymah/cipmap), I discovered that the application's backend infrastructure lacks basic security authentication.

Consequently, the names, email addresses, location, and specific project and political feedback of every resident who participated in this survey have been - and remain - publicly accessible to anyone with basic technical knowledge.

Nature of the Breach: My forensic analysis confirms that the application's API endpoints and administrative logs were left wide open.

This exposure includes:

- **Personally Identifiable Information (PII):** A database of constituent full names, email addresses, location coordinates, positive or negative votes, and full comments are exposed to the world. While the data does not explicitly list street addresses, these coordinates are precise enough to be easily cross-referenced with public property records (iMAPS) to identify specific resident homes. For residents who voted and/or left comments, their names are directly tied to their project opinions (via vote and/or comment) which are sometimes on sensitive, political topics, significantly elevating the potential for harassment, retaliation, or neighbor disputes.
- **Active and Expanding Data Collection:** The original survey has been moved to a different URL parameter and remains open for participation. Additionally, the primary domain has been replaced with a new "current projects" interface that also allows for additional voting and comments increasing the reach of the exposure. Both systems share the same unsecured backend infrastructure. This means Council Member Mahaffey is not only failing to remediate the original exposure; he is actively expanding it by collecting new resident data through the same vulnerable system.
- **Unsecured Admin Access:** Publicly accessible logs revealing administrative actions, user IDs, and metadata remain visible.

Evidence of Deletion: I should note that Council Member Mahaffey has already begun deleting files from the public repository. A static file containing PII - including administrative logs and user metadata - was removed in a recent commit. However, this deletion is recoverable through the repository's version control history (very easily accessible by anyone), and I have preserved a copy. This makes the litigation hold request below particularly urgent: deletion of evidence is already underway.

Preservation of Records: Given the gravity of this exposure and the involvement of an elected official using private infrastructure for public business, I formally request that the Town issue a Litigation Hold to Council Member Mahaffey. He should be instructed to preserve all server logs, source code, and database snapshots in their current state. Any alteration or deletion of this data subsequent to this notice could constitute the destruction of public records.

Custody of Evidence: To protect the privacy of my neighbors, I have secured forensic copies of the exposed data in an encrypted, offline archive. I will not be releasing the raw files to the public. However, I am prepared to transfer these files to the Town Attorney via secure means to assist in your internal investigation and remediation efforts.

Publication Timeline: Due to the immediate risk to resident privacy, The Peak Weekly will run a brief "Security Alert" in Thursday morning's newsletter advising residents that their data may have been compromised. I am withholding the full investigative details, including concerns about data integrity and conflicts of interest temporarily to allow the Town time to secure the breach.

I would appreciate confirmation of receipt and an initial response regarding remediation steps by end of business Thursday 1/15/26.

My goal in reporting this directly to you is to ensure the safety of this data is prioritized immediately. This is a serious failure of digital governance, and I trust the Town will act swiftly to protect its residents.

Respectfully,

Adam Whitaker | Publisher
The Peak Weekly
(919) 756-3736
www.ThePeakWeekly.com