Summary from Investigation

- SIFT so far has examined 38,935 Deleted Files that were recovered from Town's Desktop computer out of the 1.9 million files recovered by SIFT
- Findings include: Intentionally hiding Town's information in private (non-town owned) files with Town files stored on privately owned storage
- Jim Walter was an "official" user on Town's computer (not official contractor for the town)
- Many remote devices were connected to the Town's computer
    - Remote access at any time, back door access was open
- Many user accounts were found, 16 so far were discovered
- Found virtual machines
    - Why is it being done in ways that can be hidden?

Note:
Although there are legitimate uses for virtual machines, fraudsters can use virtual machines (VMs) on computers to "cloak" their identity by simulating different devices and operating systems, allowing them to create multiple accounts, bypass detection systems, and commit various types of online fraud like account takeover, credit card fraud, and identity theft, all while appearing to be legitimate users from different locations and devices; essentially hiding their real identity behind a virtual facade.

- 5 large, encrypted files were found on Town's Computer and evidence shows they were deleted
    - Why were they there?
    - Why were they deleted?
- At least 2 operating systems were found on the Town's Desktop Computer – highly unusual
- Town budget files on the Town Computer were deleted
- Discovered files called "Fudge Factor" that were deleted, and other files also labeled "Fudge Factor" were purposely retained
- Unauthorized digitization of official signature of Town Chairman
    - Unauthorized digitization of signature found labeled "original" and "replacement"
    - Deleted Unauthorized digitization of signature in timeframe that is linked to other significant events
- Former Town Employee had access and usage to Town's Microsoft 365 account after term ended
- Spreadsheets of Town's Cash flow were found on Former Town Employee's personal One Drive: Note: it is subject to open records request with Town Files on personal property
- Timing: Files were deleted on Town's Desktop Computer, after an election, in which results of the election were unknown

- Deletion, removal and destruction of Town's Computer explicitly showed that Dell was directed by Jim Walter to dispose of the hard drive after express direction of Town Board to immediately return Town's Computers intact
- Many files on Town's Computer were deleted regarding absentee ballots
- File(s) was discovered with hundreds of passwords
- Discovered use of Town's Computer for campaigning and soliciting votes
- In conclusion, the Town paid for an investigation by SIFT, the Special Investigations and Forensic Technologies Company, to examine the Town's Computers. Deleted and encrypted files unable to be opened previously, by law enforcement, were retrieved by SIFT. So far, they examined 38,935 deleted files that they recovered from Town's computers out of 1.9 million files that SIFT recovered through their investigation. The results conclusively show that the investigation needs to continue to be pursued.

- How can Town property be disposed of without consequences?
- SIFT is on standby waiting to do further analysis and work with the Sheriff's Office and DOJ. After the hard drive was opened by the DOJ the same data that SIFT reviewed and is reported here was previously reviewed by the Sheriff's Office. The Sheriff's Office said they would bring charges if any information was found. Incredibly, at that time, the Sherrif's Office found nothing to pursue or investigate further. Let's look further in the interest of good government. Citizens are now informed and our government needs to take appropriate action, as this is warranted by the revelations of this initial SIFT investigation.