Dominion Voting Machines Allowed Election Tampering: Forensic Experts

Two cyber experts examined the hard drive from a Dominion voting machine used in Colorado for two elections (November 2020 and April 2021.)[1] These independent experts determined that ***software on the machine had performed secret operations that manipulated ballot data***. Here are the key findings:

- In both elections, after vote-counting was underway, **thousands of ballots that had already been counted were secretly *re*-processed** inside the voting machine.
- In violation of federal and state law, the machine had an internal Wi-Fi adapter allowing Internet connectivity.[2] This **opens the door for virtually any computer with Internet access, anywhere in the world, to connect to the software and server**.
- The hard drive shows that, in both elections, two **new "shadow" databases were secretly created** on the machine after counting began, either through "hacking" or pre-set algorithms.
- The hard drive shows that copies of digital records of select batches of **already-counted ballots were moved over to these shadow databases without notice to election officials or judges** (including 20,346 of 25,913 ballots in 2020 and 2,974 of 4,458 ballots in 2021).
- The machine performed an **unauthorized, digital recount** on the files in the new databases.
- The machine **made only the digitally *re*-processed ballot files visible to local election officials and hid the original (not re-processed) ballot files**. The final vote count in the election exceeded the number of ballots that were made visible to the officials.
- The percentage of ballots the machine flagged for further (human) evaluation was significantly different in the *secret recount* than it had been in the *original count*, indicating that **the re-count was processed differently** than the original count.
- Dominion only recorded vote tabulations in a single location. This means that **if vote counts were to be changed, there would remain no record of the original votes in any other location and, therefore, no means of detecting the vote changes**. Additionally, the software code allows votes to be altered on any ballot.
- The machine was programmed to **erase critical logs within just a few days**, including the original vote tabulations (prior to the creation of shadow databases), activity logs, and logins, making it **impossible to identify any occurrences of unauthorized access**, software installation, network connections or other unauthorized activity.
- Dominion (as well as the Colorado Secretary of State) **destroyed all data on the hard drives of Colorado's voting machines 1 month after the April 2021 election** (as part of Dominion's required software update, referred to as the "Trusted Build"), even though *state and federal law require election records to be preserved for at least 22 months.*[3]

---

[1] The county clerk for Mesa, County, Colorado, Tina Peters, copied the hard drive from the Dominion voting machine both before and after Dominion's required software update (referred to as the "Trusted Build"), unbeknownst to Dominion or Colorado Secretary of State. Peters submitted the copies to forensic experts for examination.

[2] Seven machines in the system were found to have these adapters installed.

[3] It is believed that the same thing happened on Dominion machines in Maricopa County, Arizona, where auditors found that 284,412 ballot images were corrupted or missing and "all the data in the database related to the 2020 general election had been fully cleared" contrary to federal law.