Sequoia, Smartmatic, & Venezuela

- **Sequoia Voting Systems** got its start in the early 1970's as **Mathematical Systems Corporation** of Anaheim, California, which offered an alternative punch-card voting system to Votamatic[1].
- A couple of years later, MSC was acquired by the **Diamond National Corporation**, part of the Diamond Match Company[2].
- In 1983, Diamond rebranded their punch card voting business as **Sequoia Pacific Systems Corporation**. They would eventually become one of the largest providers of electronic voting systems in the United States.
- In 2005, Sequoia was acquired by **Smartmatic Corp.**[3], which led to a significant amount of scrutiny at the time. The Venezuelan-owned company was selected the previous year in 2004 by the **Chavez-era Venezuelan government** "to provide the voting machines system for the presidential recall election, even though it would have been the company's **first time providing machines for an election**.[4]"

The New York Times

WASHINGTON

U.S. Investigates Voting Machines' Venezuela Ties

By TIM GOLDEN OCT. 29, 2006

The federal government is investigating the takeover last year of a leading American manufacturer of electronic voting systems by a small software company that has been linked to the leftist Venezuelan government of President Hugo Chávez.

1 https://web.archive.org/web/20181022183528/https://www.verifiedvoting.org/resources/voting-equipment/ess/votamatic/
2 Founded in the 1850's by Edward Tatnall after his friend taught him to make matches. http://www.matchpro.org/
3 https://web.archive.org/web/20181023142328/http://www.sequoiavote.com/pressText.php?pressIn=41
4 https://web.archive.org/web/20180608221821/https://www.nytimes.com/2006/10/29/washington/29ballot.html

- From the *New York Times*[5]:
  - "The inquiry is focusing on the Venezuelan owners of the software company, the Smartmatic Corporation, and is trying to determine whether the government in Caracas has any control or influence over the firm's operations, government officials and others familiar with the investigation said."
  - "The concerns about possible ties between the owners of Smartmatic and the Chávez government have been well known to United States foreign-policy officials since before the 2004 recall election in which Mr. Chávez, a strong ally of President Fidel Castro of Cuba, won by an official margin of nearly 20 percent."
  - On top of that, Smartmatic teamed up with a software company called Bitza which Chavez's government owned a 28% stake in[6].
  - "Opposition leaders asserted that the balloting had been rigged. But a statistical analysis of the distribution of the vote by American experts in electronic voting security showed that the result did not fit the pattern of irregularities that the opposition had claimed."
- Despite the American expert's claims that the electronic voting security didn't suggest any fraud had occurred, a CIA expert would later testify in 2009 that he believed Chavez and his allies did in fact fix the 2004 election recount[7].

5 https://web.archive.org/web/20180608221821/https://www.nytimes.com/2006/10/29/washington/29ballot.html
6 https://web.archive.org/web/20180926234107/https://maloney.house.gov/media-center/press-releases/smartmatic-announces-sale-sequoia-voting-systems
7 https://web.archive.org/web/20180223031327/http://www.mcclatchydc.com/news/politics-government/article24530650.html

- Stigall told the Election Assistance Commission that computerized electoral systems can be manipulated at five stages, from altering voter registration lists to posting results.
- "You heard the old adage 'follow the money,' " Stigall said, "I follow the vote. And wherever the vote becomes an electron and touches a computer, that's an opportunity for a malicious actor potentially to . . . make bad things happen."
- Stigall did not address any concerns about US elections because he wasn't speaking for the CIA, but he did say that most web-based ballot systems had proved to be insecure.
- The commission was criticized for giving states more than $1 billion to buy electronic equipment without first setting any performance standards. **Numerous computer-security experts concluded that U.S. systems can be hacked**, and allegations of tampering in Ohio, Florida and other swing states triggered a campaign to require all voting machines to produce paper audit trails.
- "The CIA got interested in electronic systems a few years ago," Stigall said, "after concluding that foreigners might try to hack U.S. election systems." He said he couldn't elaborate "in an open, unclassified forum," but that any concerns would be relayed to U.S. election officials.

- Smartmatic owned Sequoia until 2007, when the Treasury Department's Committee on Foreign Investment launched an investigation. In November of that year, Smartmatic quickly sold Sequoia[8] to a group of investors let by their US-based management team, which ended the inquiry.

8 https://web.archive.org/web/20180926234107/https://maloney.house.gov/media-center/press-releases/smartmatic-announces-sale-sequoia-voting-systems

- Despite the sale, it came to light that Smartmatic continued to own the software that counts votes on Sequoia voting machines, and licenses to Sequoia that software, which Smartmatic develops in Venezuela[9].
- In 2007, a computer security group at UC Santa Barbara was asked to analyze the security of Sequoia voter machines. The report found "a number of serious security issues that could be "exploited by a determined hacker to modify (or invalidate) the results of an election" and that could "be carried out without any knowledge of the source code[10]."
  - "An analysis of the source code by Matt Blaze and others at UC Berkeley found that "the Sequoia system lacks effective safeguards against corrupted or malicious data injected onto removable media, especially for devices entrusted to poll workers and other temporary staff with limited authority…[11]"
  - "Many of the security features of the Sequoia system, particularly those that protect the integrity of precinct results, employ cryptography" that is "easily circumvented."
  - The researchers concluded that "virtually every important software security mechanism is vulnerable to circumvention[12]."
  - California withdrew approval for the use of Sequoia machines, but then granted re-approval for the use of Sequoia's machines subject to various conditions[13].

9 https://web.archive.org/web/20181023142341/https://www.nist.gov/sites/default/files/documents/itl/vote/SequoiaSmartmaticReport61208.pdf
10 https://web.archive.org/web/20180526075628/http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/red-sequoia.pdf
11 https://web.archive.org/web/20180526075628/http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/sequoia-source-public-jul26.pdf
12 https://web.archive.org/web/20180526075628/https://www.wired.com/2007/08/ca-releases-sou/
13 https://web.archive.org/web/20180526075628/http://www.govtech.com/security/California-Decertifies-Voting-Machines-Conditions-Applied.html

- Thirteen other states states continued using Sequoia machines as well[14].
  - One of those states was New York, which in 2008 revealed that it had "found problems with 50 percent of the roughly 1,500 ImageCast optical-scan machines (shown in the video above) that Sequoia Voting Systems has delivered to the state so far[15]…"
- The year before, Sequoia was identified as the company that had supplied the notorious faulty punch cards during the 2000 election—the very punch cards that led Congress to pass legislation moving the country away from punch cards and toward electronic voting machines. Several former workers told Dan Rather that Sequoia had changed the paper stock before the election and knew in advance the punch cards would cause problems[16].
- **Important:** Nearly twelve years later, the CEO of Smartmatic would admit that the numbers seemed manipulated and tampered with in the 2017 election in Venezuela. He mentions that in order for Smartmatic to catch votes being tampered with, **there must be fair audits with both political parties present**[17].
  - "It is imporant to point out that this would not have occurred if auditors of all political parties had been present at every stage of the election."

14 https://web.archive.org/web/20180526075628/https://www.theverge.com/2012/11/6/3609506/voting-machine-electronic-voting-history-in-america
15 https://web.archive.org/web/20180526075628/https://www.wired.com/2008/07/ny-50-percent-o/
16 https://web.archive.org/web/20180526075628/https://www.wired.com/2007/08/sequoia-voting/
17 https://youtu.be/5RQDxfBXnnM