FRANK ASKIN, Esq.
PENNY M. VENETIS, Esq.
RUTGERS CONSTITUTIONAL LITIGATION CLINIC
123 Washington Street
Newark, New Jersey 07102
(973) 353-5687
Attorneys for Plaintiffs

Assemblyman Reed Gusciora, Stephanie Harris, Coalition for Peace Action, and New Jersey Peace Action, Plaintiffs, v. Jon Corzine, Governor of the State of New Jersey (in his official capacity) and Nina Mitchell Wells, Secretary of State of the State of New Jersey (in her official capacity), Defendants.	SUPERIOR COURT LAW DIVISION MERCER COUNTY Docket No. MER-L-2691-04 CIVIL ACTION

CERTIFICATION OF DECEMBER 1, 2008

ANDREW W. APPEL, being of full age, hereby certifies:

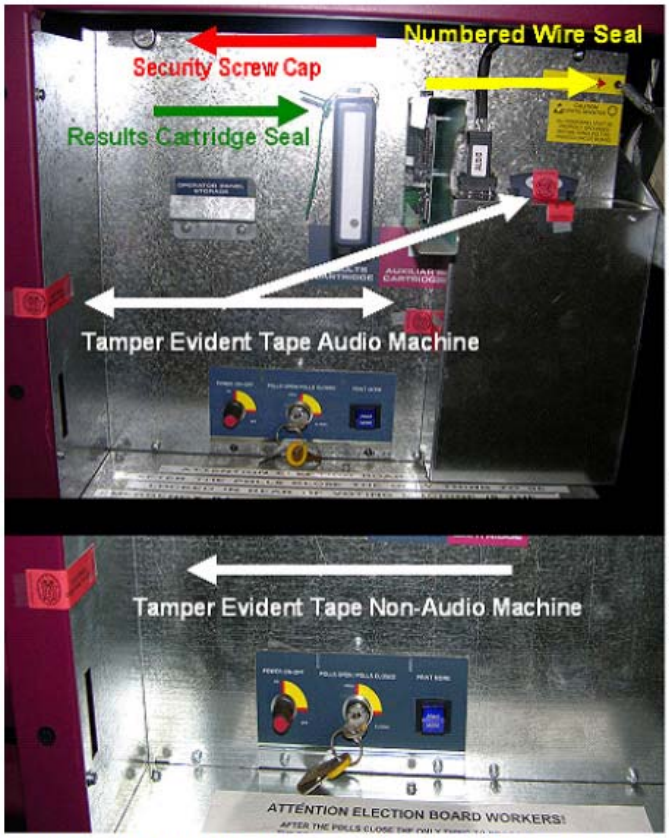
1. I am a Professor of Computer Science at Princeton University. I have been qualified as an expert in this case.

2. When I examined two voting machines from Union County, New Jersey in July 2008, the only security seal on those machines was a plastic strap seal in the holder for the Results Cartridge. This seal was present on one machine but not the other. In my expert report of August 29,

2008 (and in my video delivered with it) I demonstrated that the strap seal does not prevent removal of the circuit-board cover, and therefore does not prevent replacement of the ROM chips to install fraudulent vote-stealing firmware.

3. In October 2008 I learned that New Jersey intended to install additional tamper-evident security seals on its AVC Advantage voting machines.

4. In October 2008 Sequoia Voting Systems posted onto its website a “Response from Sequoia Voting Systems to the Report of Andrew W. Appel.” That document was presented to the Court in September. In that document, Sequoia recommends a particular set of seals to be installed on its voting machine, and shows a photograph of how the seals are to be installed. (Photograph reproduced on next page.)



TECHNICIAN'S INSTRUCTIONS

ALL MACHINES

Security Screw Cap (upper left hand corner) Insert screw into back of cap. Place numbered cap over screw. ***Record number***.

Numbered wire seal (upper right hand corner) Insert numbered wire seal. Lock seal and remove excess wire. ***Record number***.

Results cartridge seal – Insert plastic numbered seal. ***Record number***.

AUDIO MACHINES

Tamper evident tape (3 pieces)

1. Left hand side-place a piece of tamper evident tape from the e-box to the metal shroud horizontally.
2. Place tamper evident tape horizontally from metal shroud to side of audio box.
3. Place tamper evident tape over audio cartridge and onto audio box vertically. ***Record number***.

NON-AUDIO MACHINES

Tamper evident tape (1 piece)

Left hand side- place a piece of tamper evident tape from the e-box to the metal shroud horizontally.

Figure 3: New Jersey's instructions for proper sealing of the AVC Advantage.

(Figure 3 from Sequoia's Document)

5. On November 4th, 2008, on Election Day, as a member of the public, I observed the closing of the polls at Princeton Township Election District 9. There I saw that the same seals were installed on the two voting machines that I observed. On the same evening of November 4th, other faculty and students from Princeton University observed the closing of the polls at other Election Districts in Princeton, NJ. I had instructed these observers what to look for (using the picture from

Sequoia's web site as a guide), and they all reported seeing the seals in the same configuration.

6. On November 13, 2008 I received by delivery to my office, sent from Deputy Attorney General Jason Postelnik, samples of seals that New Jersey proposed to install on its voting machines.[1]

7. These are all consistent: My personal observation of the voting machines in use on November 4th, the observations of others who reported to me what they saw on election night in other voting precincts, the photograph from Sequoia's web site, and the seals mailed to me by Mr. Postelnik. Therefore I conclude that the State of New Jersey did install these seals, of the kind sent to me by Mr. Postelnik, on at least some voting machines before election day, in the configuration described by Sequoia.

8. As an expert in computer security, I have studied the interaction of physical security (such as seals) with computer security (such as installation of fraudulent computer programs). However, I have not had much direct experience with the physical manipulation of seal devices. Even though I am unpracticed with physical seals, I found that with very little analysis and

[1] Letter dated November 12, 2008, from Jason S. Postelnik to Andrew W. Appel; cc'd to the Court.

practice, using tools from my home workshop, I was able to defeat all four of the seals currently used by the State of New Jersey on its AVC Advantage voting machines.

9. I have prepared a 20-minute video showing the basic techniques for defeating these seals. In the video I demonstrate how the seals are installed, and how an attacker can remove them and reinstall them without leaving visible evidence. These seals are meant to prevent the undetected removal of the circuit board cover. Under this cover are the ROM chips whose replacement can cause the voting machine to fraudulently transfer votes from one candidate to another. I demonstrate that someone like myself, who has had no previous practice defeating seals, can remove and replace these seals in minutes. I estimate that someone with more practice could do it even faster.

10. I shot the video in a room at Princeton University, using a Sequoia AVC Advantage voting machine that I purchased in 2007. It has the same physical configuration as any New Jersey AVC Advantage that does not have an audio kit installed. The configuration of the audio-kit machines is quite similar. My general conclusions apply to the audio-kit configuration as well.

11. **The seals.** New Jersey now uses four seals:

a. A cup seal, also known as a security screw cap, used on one of the 10 screws that hold the circuit-board cover in place.

b. A wire rope lock seal, looped through a hole in the circuit board cover and a corresponding hole in the circuit board enclosure.

c. Security tape, which is supposed to show the words “OPEN VOID” if removed and replaced, taped to both the circuit-board cover and the cabinet of the AVC Advantage.

d. A plastic strap seal holding the Results Cartridge in place.

On the video I demonstrate the defeat of all four of these seals.

12. **Cup seals.** The security cap screw has two main components: the base and the cap.

First a screw is inserted through the hole in the base; then the screw goes through the hole in the circuit-board cover; then into the circuit-board enclosure. This screw is tightened down, so it holds both the seal base and the

circuit board cover down to the enclosure. Then the cap is pressed into place. The cap has a serial number stamped or engraved into it. Supposedly one cannot remove and replace this seal without leaving evidence of tampering.

13. In fact, I found at least two different ways to defeat this seal. The simplest way is to insert a screwdriver between the cap and the base, and simply pry the cap off. This destroys the base, but leaves the cap undamaged. This method leaves no marks on any other component of the voting machine.

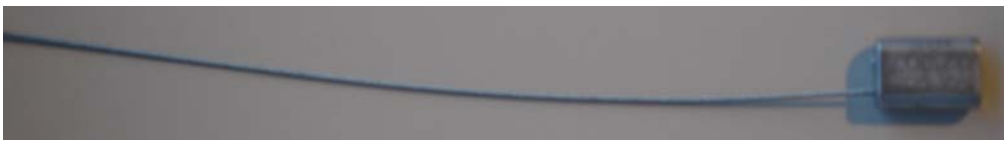
14. The cap is the only component (of the cup seal) with a serial number. These cup seals are offered for sale by their manufacturer, American Casting, for 75 cents each. Therefore it would be easy for an attacker to bring a new replacement base, to use with the existing serial-numbered cap. When I demonstrate this on the video, it took me 100 seconds. I believe that with practice, using the right-size screwdriver, I could reliably do it in 10 seconds.

15. To reinstall the seal, the spring clip must be removed from the inside of the cap; the first time I did this it took about 30 seconds. Then, to reinstall the seal, I

simply press it into place; this takes about 7 seconds on the video.

16. I have found another way to defeat this seal that does not even require the attacker to have a supply of fresh base components. I take a piece of aluminum roof flashing (like a very thick aluminum foil) and roll it to the ¾-inch diameter of the seal cap, so that it fits between the cap and the base. I then hammer it into place, and twist it off. This removes the cap without damaging the external part of the base. The internal part of the base, containing the spring clip that holds the cap in place, comes off with the cap. Then the base can be easily removed, and reinstalled later. To reinstall the cap (with its spring clips), a dab of superglue will suffice. The result is indistinguishable from the originally installed seal. However, to do this reliably I would need more practice and experimentation. I do not show this method on the video attached to this certification.

17. **Wire rope lock seal.** The wire rope lock seal has a metal component that looks like a padlock, and a long braided steel cable.



In use on the AVC Advantage, the cable is threaded through a hole in the circuit board cover and one in the enclosure underneath, tying them together. Then the cable is pushed through hole in the “padlock”. Inside the padlock there are ball bearings and a spring, in a configuration that makes it “impossible” to pull the wire back out.

18. I have found that this seal is quickly and easily defeated. The base of the “padlock” has two little holes. By threading a #4 wood screw though a hole, one can yank out the entire base with a pair of pliers. This leaves almost no marks at all on the base, and absolutely no marks at all on the serial-numbered padlock. When the base is removed, the internal components (balls and spring) can be removed. Then the cable easily comes out. On the video I demonstrate this in 50 seconds. Later, the padlock can be reassembled, and the base can be pressed into place. This leaves the cable lock seal as good as new, easily reinstalled.

19. The cable lock seal can be used in either of two configurations.

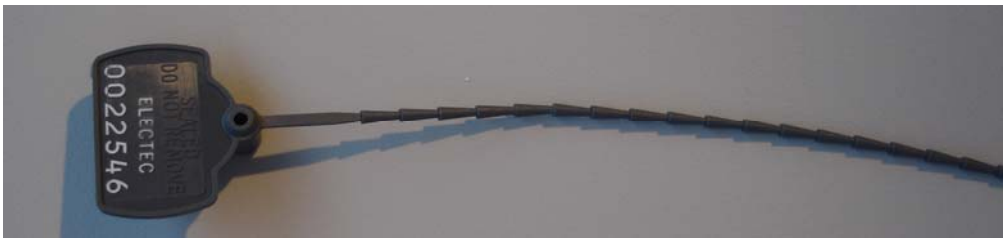
    a. In the first configuration, one pulls the cable through the padlock, and one leaves the end of the

cable untrimmed. On the videotape I demonstrate the defeat of this method.

b. In the second configuration, after the cable is pulled through the padlock, one cuts off the extra cable. This makes the end of the cable fray. One might think that, after removing the padlock, the frayed cable cannot be reinserted all the way through the padlock. But this is not the case: I have been able to defeat this configuration as well. While the padlock is in its disassembled state, I have found that I can twist the frayed cable end together enough to feed it through. The trick is to pull the wire through the different components of the padlock before reassembling the padlock. However, to do this reliably I would need more practice and experimentation. I do not show this method on the video attached to this certification.

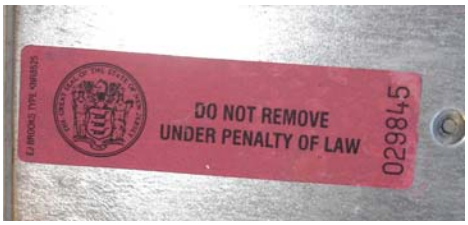
20. Thus, the padlock seal is easy to remove and reinstall with simple tools, in either of these two configurations.

21. **The plastic strap seal.**



The first time I attempted to defeat a plastic strap seal, using a simple jeweler's screwdriver, it took me less than 20 seconds. With practice, I think I could do it in 5 seconds. This leaves the seal uncut, ready to reinstall. On the video, I reinstalled this seal in about 8 seconds. After the seal is reinstalled, it would be difficult to see that anyone had tampered with it.

22. **The tamper-evident tape.**



(as first installed)

(after naïve peeling)

Although I have not had previous experience removing tamper-evident tape, I have in the past removed bumper stickers from my car. The way to do that cleanly is with a hair dryer or a heat gun. (A heat gun is just like a blow dryer for hair.) Based on this practical

experience, I applied a heat gun to the tape seal. This softens the adhesive enough so that I can remove the seal (using a single-edge razor blade), and later replace it, without any evidence of tampering. The letters “VOID” or “OPEN” do not appear. I found that 80 seconds application of heat was sufficient, followed by 40 seconds of carefully peeling off the tape. Thus, it took 2 minutes to remove the tape. Reinstalling the tape later is simple: one just presses it down. This takes about 2 seconds.

23. As I explained in my expert report of August 29, 2008, experts on physical security have published papers in the scientific literature on physical seals, encompassing all the general kinds that I am writing about today. These authors report that all such seals can be easily and cheaply defeated in minutes or less. Therefore I was not surprised that it could be done. However, those authors do not disclose anything about the methods they used.

24. I found that it was easy to devise workable methods for defeating any of the seals. After studying the seals in my basement for a few hours, I was ready to attempt defeating them on an actual voting machine.

25. I videotaped my first experiments with the seals as installed on an actual voting machine. The raw footage

is approximately 40 minutes. That footage contains experiments with all the methods described in this certification. From this I made the 20-minute video that shows the seals, shows the installation of the seals, and show basic methods of removing and replacing the seals.

26. The 4 seals installed by the State of New Jersey on its AVC Advantage voting machines can be all removed, and later replaced, by someone who has had almost no previous practice, in less than 7 minutes. This is what I show in the video accompanying this certification.

27. In addition to this 7 minutes, the rest of the “hack” (picking the lock, removing screws, replacing the ROM, replacing screws) takes 7 minutes, as I demonstrated in the video that accompanied my expert report of August 29, 2008.

28. I estimate that someone with more practice, who is “hacking” his 20th voting machine, could defeat these same 4 seals in a total of 2 minutes.

29. In my opinion, the security seals installed by the State of New Jersey in September 2008 do not significantly protect the AVC Advantage against fraudulent replacement of program ROM chips, or against other attacks that require access to the motherboard of the voting machine.

30. I certify that the foregoing statements are true. I am aware that if any statements are willfully false, I will be subject to punishment.

_____

Dated: December __, 2008 Andrew W. Appel
Princeton, New Jersey