Declaration of Stephen Spoonamore

740 Quinby Ave.
Wooster OH 44691

1. I am a recognized expert in the field of electronic data security and digital network architecture.

2. I have agreed to serve as an expert witness for the plaintiffs in the case of King Lincoln Bronzeville Neighborhood Association before the United States District Court in Columbus, Ohio.

3. I have served as the CEO and/or CTO of companies engaged in the design and development of digital systems. Including: CPR Group Inc., Cybrinth LLC, DuosTech Inc., SWN Communications, FreePlay Inc. and GSP inc.

4. I have served in industry leadership positions in a number of professional organizations in the field of electronic data security and commerce, including but not limited to: Board Member of the AFEI (Association For Enterprise Integration) and Task Force Chairman, NECCC (National Electronic Commerce Coordination Commission) to establish digital identity rules for State Government Systems.

5. Digital Systems I have designed or consulted upon are currently serving to secure elements of: MasterCard, American Express, Chubb insurance, Bloomberg, Boeing, NBC-GE, NewsCorp, the US Department of Energy, The US Navy, The US Department of State and Other Government Agencies.

6. Because of my interest in data security and in democracy, I have followed with interest the security issues involved with electronic voting in United States. My understanding of the vulnerabilities of American elections to fraudulent manipulation is based upon conversations with professionals in election administration working within state governmental structures as well as information technology specialists working in private industry on a contract basis for state governments.

7. I have agreed to function as an expert resource and witness for plaintiffs' counsel and the King Lincoln case in federal court in Ohio.

8. The opinions expressed below are held by me to a reasonable degree of certainty as understood within my professional area of expertise in the detection and prevention of fraud in data processing systems.

<u>In regard to the system set up to tabulate the vote in Ohio in 2004.</u>

1) The vote tabulation and reporting system, as initially designed, was supposed to allow each

county central tabulator (Computer A) to add up local information locally, and then, via a lightly encrypted system, send the information to the Sec. of State statewide tabulator (Computer B). This system, while using public Internet and public information carrying capacity, could be compromised at the level of one county (Computer A is hacked) or in the transmission of any one county to the central state tabulator (Computer A talking to Computer B). However, it would only be possible to compromise the vote on a statewide basis by a compromise at the state level tabulator (Computer B is hacked). Alternately I have been told that these processes were replaced at the last minute by fax transmitted results. It is relatively simple to establish if the security of the transmissions, whether sent by fax, or by electronic transmission, by reviewing the network architecture as operated on election night, and review the session logs of the secretary of states central tabulation computer to determine the IP address and times of communication by other machines to the the Secretary. The variable nature of the story of what occurred, and lack of documentation available, would be cause to launch an immediate fraud investigation in any of my banking clients.

2) The vote tabulation and reporting system, as modified at the direction of Mr. Blackwell, allowed the introduction of a single computer in the middle of the pathway. This computer located at a company principally managing IT Systems for GOP campaign and political operations (Computer C) received all information from each county computer (Computer A) BEFORE it was sent onward to Computer B. This centralized collection of all incoming statewide tabulations would make it extremely easy for a single operator, or a preprogrammed single "force balancing computer" to change the results in any way desired by the team controlling Computer C. In this case GOP partisan operatives. Again, if this out of state system had ANY digital access to the Secretary of States system it would be cause for immediate investigation by any of my banking clients.

3) If scenario #2 described above is true, Computer C, was placed functionally in a central control position in the network, for Computer C to have even updated instructions for various tabulators at the county level (Computers A) to change their results at the county level. If this had happened, in order to cover up this fact, the hard drives of the county level tabulators would have to be pulled and destroyed, as they would have digital evidence of this hacking from Computer C. The efforts by the company in charge of these computers to pull out hard drives and destroy them in advance of the Green Party Recount from the 2004 election is a clear signal something was deliberately amiss with the county tabulators (Computers A). If even the presence of such a Computer C was found in a banking system, it would be cause to launch an immediate fraud investigation.

-This computer placement, in the middle of the network, is a defined type of attack. It is called a MIM (Man in the Middle) Attack. It is a common problem in the banking settlement space. A criminal gang will introduce a computer into the outgoing electronic systems of a major retail mall, or smaller branch office of a bank. They will capture the legitimate transactions and then add fraudulent charges to the system for their benefit.
-Another common MIM is the increasingly common "false" website attack. In this MIM, errors in the computers that feed the Digital Name Service are exploited directing an unsuspecting user

to a site that looks like the one they wished to visit, but is in fact an "evil twin" which then exploits them for various purposes for a portion of the time, and then in many cases passes them on the CORRECT web site they wanted. Once passed on, the operators of the evil twin site may continue to exploit the user, or later duplicate the session and exploit them in another manner.

-Any time all information is directed to a single computer for consolidation, it is possible, and in fact likely, that single computer will exploit the information for some purpose. In the case of Ohio 2004, the only purpose I can conceive for sending all county vote tabulations to a GOP managed Man-in-the-Middle site in Chattanooga BEFORE sending the results onward to the Sec. of State, would be to hack the vote at the MIM.

IN REGARD TO THE DIEBOLD SYSTEMS, Formerly Global, DESI and now called Premier.

In my opinion, there is NO POSSIBLE WAY to make a secure touch screen voting system. None. Secure systems are predicated on establishing securely the identity of every user of the system. Voting is predicated on being anonymous. It is impossible to have a system that does both. It is possible to design relatively secure optical scan machines, but even these can be hacked in even the best of cases. In the case of optical scan you have the ability to recount manually the paper ballot itself, and the ability to spot check the machines for errors against a sample of hand recounting.

Even considering no secure system for touch screen machines can be designed, ever, the Diebold system is riddled with exploitable errors. The SAIC report on the system architecture, commissioned by Maryland Gov. Erlich, outlined over 200 concerns. Many of these concerns are almost comical from the perspective of a computer architect. One example of this: The existence of negative fields being possible in some number fields. Voting machines as custom built computers which should be designed to begin at the number Zero, no votes, and advance only in increments of 1, one vote, until they max out at the most possible votes cast in one day. Perhaps 3000 voters could use a machine in one day, but more realistically 400 or so. There is no possible legitimate reason that NEGATIVE votes should ever be entered. And yet these machines are capable of having negative numbers programmed in, injected, or preloaded.

IN REGARD to Mr. Mike Connell.

Mr. Connell and I share a mutual interest in democracy building, freedom of speech and religion worldwide. We have mutually participated in activity to forward this goal. At a meeting in London last year, and again at a Lunch in Washington, DC, Mike and I briefly discussed voting security. While he has not admitted to wrongdoing, and in my opinion he is not involved in voting theft, Mike clearly agrees that the electronic voting systems in the US are not secure. He further made a statement that he is afraid that some of the more ruthless partisans of the GOP, may have exploited systems he in part worked on for this purpose. Mr. Connell builds front end applications, user interfaces and web sites. Knowing his team and their skills I find it unlikely they would be the vote thieves directly. I believe however he knows who is doing that work, and has likely turned a blind eye to this activity. Mr. Connell is a devout Catholic. He has admitted

to me that in his zeal to 'save the unborn' he may have helped others who have compromised elections. He was clearly uncomfortable when I asked directly about Ohio 2004.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 17th day of September 2008.

Stephen Spoonamore