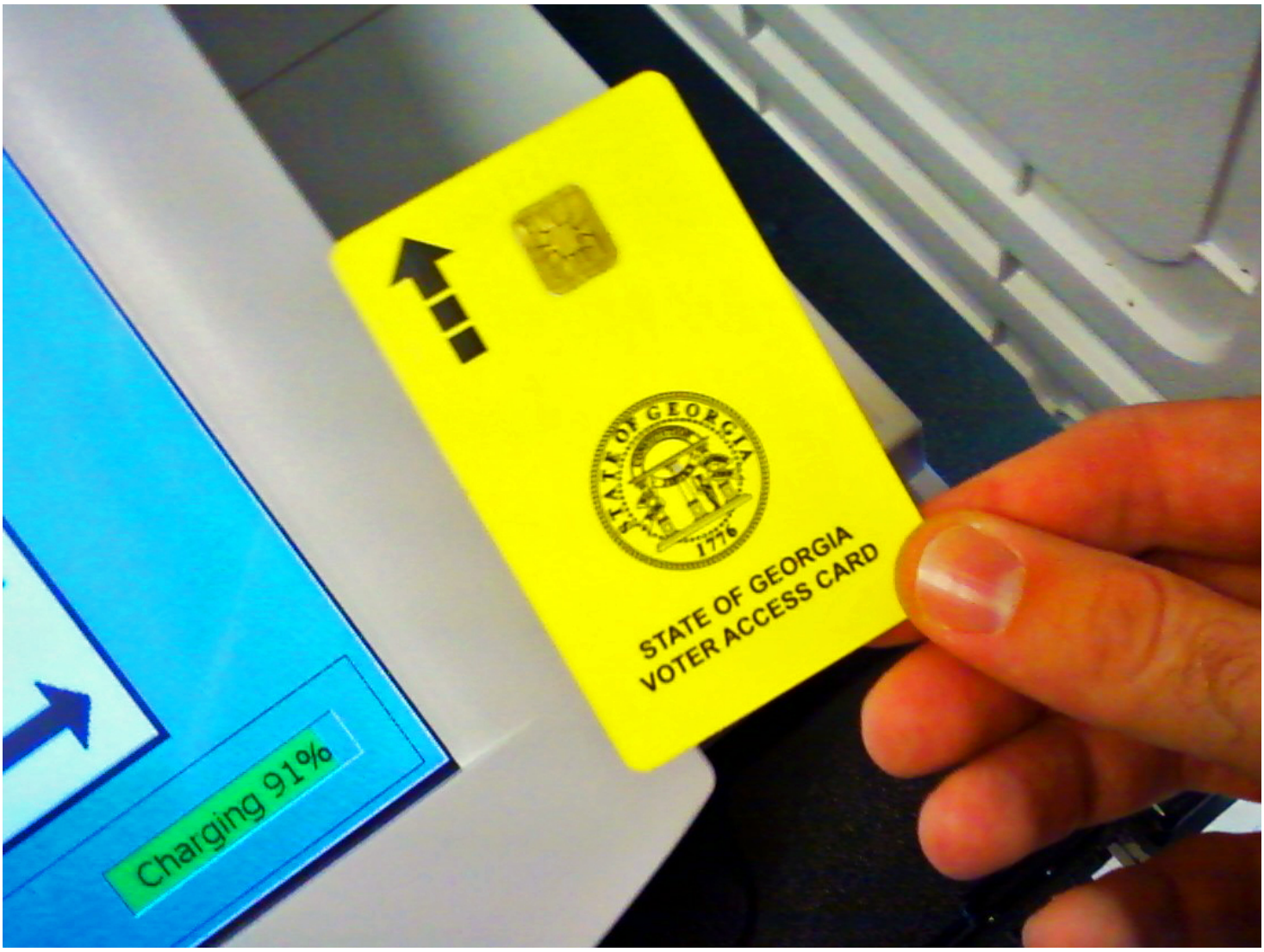
PART FOUR

CITIZEN SLEUTH EXPOSES SHOCKING FAULTS BUILT INTO DIEBOLD ELECTION SYSTEMS



A voter uses the voter access card for a Diebold voting machine in Georgia. The entire state uses unauditable touchscreen voting machines with known vulnerabilities. The Diebold machines were implicated in the 2002 Senate race in Georgia in the suspicious defeat of Vietnam veteran Max Cleland. PHOTO: Jason Riedy (CC).

The spread of computerized voting has carried with it an enormous potential for electronic skulduggery. In 2003, Bev Harris, a citizen sleuth and the author of *Black Box Voting: Ballot Tampering in the 21st Century*, made a shocking and game-changing discovery: Diebold, then one of the primary manufacturers of voting machines, had left the 40,000 files that made up its Global Election Management System (GEMS) on a publicly accessible website, entirely unprotected.

Diebold was never able to explain how its proprietary tabulation program ended up in such an exposed position. Harris downloaded the files, and programmers worldwide pounced, probing the code for weaknesses. The wall of secrecy, said Harris, began to crumble.

GEMS turned out to be a vote rigger's dream. According to Harris' analysis, it could be hacked, remotely or on-site, using any off-the-shelf version of Microsoft Access, and password protection was missing for supervisor functions. Not only could multiple users gain access to the system after only one had logged in, but unencrypted audit logs allowed any trace of vote rigging to be wiped from the record.

> Diebold voting machines feature unencrypted audit logs that allow vote rigging to be wiped from the record.

The public unmasking of GEMS by an average citizen (who was not a programmer herself) served as a belated wake-up call to the world's leading computer-security experts, who finally turned their attention to America's most widely used voting systems.

Damning reports have since been issued by researchers from Johns Hopkins, Princeton, Rice, and Stanford Universities, the Brennan Center for Justice, and the Government Accountability Office (none of them institutions hospitable to tinfoil hat conspiracy theorists). Experts describe appalling security flaws, from the potential for system-wide vote-rigging viruses to the use of cheap, easily replicated keys; the same kind used on jukeboxes and hotel minibars—to open the machines themselves.

In 2005, the nonpartisan Commission on Federal Election Reform, chaired by Jimmy Carter and James Baker, stated unequivocally that the greatest threats to secure voting are insiders with direct access to the machines: "There is no reason to trust insiders in the election industry any more than in other industries."

> There is no reason to trust insiders in the election industry any more than in other industries.
>
> — Jimmy Carter and James Baker