DOUGLAS DRENKOW
Research & Communications

http://DouglasDrenkow.com/write3d.html

Backed by Big Money,
Congress May Gut Identity Theft Laws

An Article Scheduled to be Published in Core Media Weeklies
(But Published Online, in DailyKos.com, OpEdNews.com, etc.)
Week of March 23 to March 29, 2006

As I sit here writing this, my ATM/Debit Check card (from a bank of America that shall remain nameless) has been blocked. After receiving the official notice a few days ago, I hurriedly made other arrangements for my automatic payments, as for the Internet service I used to research this article and e-mail it to my editor; modern life runs on digital money.

Of what crime was I guilty, to receive such punishment? I had the gall to claim an identity. Apparently, my account (and God only knows how many more) "may have been compromised at a third-party location." I am reassured that my card is covered by "both zero liability and next day refunds guaranteed credit" (subject to dollar limits) but I am also told to carefully review my "statements and report any unauthorized transactions" ... although I may be (and indeed am) "temporarily unable to access Online Banking" (The last time something like this happened, three years ago, I caught the problem online before the bank did, and before the rent check bounced ... and I bounced out on the sidewalk). I await my new card, said to arrive within five business days ... as of a week ago.

Sound familiar? Odds are you or someone you know has suffered the same or worse fate. According to the Federal Trade Commission, there are nearly 10 million identity theft victims each year; that's about 19 every minute! Far from a victimless crime, identity theft costs the businesses, financial institutions, and consumers of America billions of dollars a year.

Earlier this year, the FTC levied the largest civil penalty on record—a $10 million fine plus a $5 million restitution fund—on ChoicePoint, a "data broker," or credit-reporting service, used by over 50,000 merchants and landlords for credit checks on potential customers and tenants: In 2005, ChoicePoint became the poster child for lax identity protection, by allowing an organized ring of identity thieves to gain access to over 160,000 personal records; hundreds of individuals became victims of identity theft.

Remember, too, that the 9/11 hijackers left behind piles of credit cards in their rooms; identity theft is a weapon of choice—a "weapon of mass financial destruction"—for Al Qaeda terrorists worldwide.

Doug@DouglasDrenkow.com · 5760 Main St., South Gate, CA 90280 · 562-531-6643 · Cell: 310-570-8930

So naturally, the federal government is doing everything in its power to crack down on this crime wave, this threat to national financial security, to ease the burden upon us innocent victims of this crime that has turned countless lives upside-down (To paraphrase the Bible, it's easier to pull a camel through the eye of a needle than it is to restore bad credit).

Don't bank on it.

The ChoicePoint debacle was brought to public attention not by some federal regulation but by the strict identity theft laws here in California, which call for notifying victims of almost any breaches in security—not just those that the financial institutions themselves determine to be "reasonably likely to result in substantial harm or inconvenience to the consumer" (as the new federal legislation would mandate)—and which freeze the accounts of potential victims: As a representative of the Consumers Union has said, "we shouldn't have to wait until an identity thief has already bought a Lexus in your name in order to have the right [to] protect yourself."

The same sort of strict reporting requirements and account freezes are found in the anti-identity-theft laws in several other states that will be gutted like a dead fish by the legislation that was just voted out of committee last week by the House Committee on Financial Services.

And to me, that stinks like a dead fish. Actually, it is the smell of money, and lots of it.

In particular, according to the Center for Responsive Politics, fourteen of the twenty members of the House who receive the most campaign contributions from the commercial banking industry—whose interests are not served by letting the public know their security has been breached, let alone by making good on the losses—serve on the House Committee on Financial Services: Eleven Republicans, including the Chairman, Michael G. Oxley (R-OH), and three Democrats.

And the six remaining House members out of the top twenty getting the largest contributions from the commercial banking industry are hardly ill-placed to influence legislation: In addition to Henry Bonilla (D-TX), the first Hispanic Republican elected to Congress from Texas, the big bank money goes to Dennis Hastert (R-IL), Speaker of the House; Roy Blunt (R-MO), House Majority Whip; Tom DeLay (R-TX), indicted former House Majority Whip; Eric Cantor (R-VA), Chief Deputy Majority Whip; and David Dreier (D-CA—representing most of the territory covered by Core Media publications), Chairman of the House Rules Committee.

In particular, the Rules Committee is notorious for keeping legislation from reaching the floor of the House, in what longtime observers have found to be the most partisan chokehold on the democratic process in memory. As the *Boston Globe* reported in its groundbreaking investigation in October of 2004 (and things have gotten only worse), "the Rules Committee, the all-powerful gatekeeper of the Republican leadership ... has sidelined legislation unwanted by the Bush administration, even when a

majority of the House seemed ready to approve it."

But who would want this current legislation, H.R. 3997 (identical to S.2129, in the Senate), laughingly called the "Financial Data Protection Act of 2005" (but I'm not laughing), just voted out of committee, to ever get that far? Who in their right mind would ever want passed what the U.S. Public Interest Group has called "the worst data security bill ever"?

Maybe those in big banking for whom it would become the best data security bill ever bought ... at all our expense.