

BUCKET FILE COPY ORIGINAL

From: Charlie M [i2cmars@yahoo.com]
Sent: Friday, August 28, 2009 11:20 AM
To: Peter Trachtenberg; Jamison Prime; fcc@bcpiweb.com; Congressman Larry Kissell
Subject: GN Docket No. 09-157 and GN Docket No. 09-51

I tried to file on www.regulations.gov --- can't get it to take

I leave it to YOU to get the job done, please.
 I DID get it to FCC as -
 Your Confirmation Number is: '2009828904600 '
 Date Received: Aug 28 2009
 Docket: 09-66
 Number of Files Transmitted: 1

FILED/ACCEPTED

SEP - 8 2009

Federal Communications Commission
 Office of the Secretary

To the FCC -
 Regarding your wireless Industry NOI - GN Docket No. 09-157 and GN Docket No. 09-51

You should be doing everything possible to make ID theft IMPOSSIBLE.

ANY new specification should include, not just 128 bit or 1,024 bit, but at least 10K bit encryption for important information such as military and medical records, with rotating encryption encoding during any transmission. These records are of VITAL IMPORTANCE to the people involved, so you should not just listen to the industry companies responsible for making the hardware and software, because they will want to COMPROMISE security for ease-of-design or ease-of-implementation. Instead, ask the people who REVIEW the industry and are critical of lax efforts, casual mistakes, and the like, for what they see as both "advised" and "required" standards. Then implement the TOUGHEST set of rules.

All personnel involved in creating and maintaining any encryption should be required to pass a Security Check of at least "Secret" level, and perhaps "Top Secret" for anyone involved in a position that can change encryption keys manually. Purposeful compromising of data should carry a mandatory jail sentence, and confiscation of any "fruits of the tree" resulting from it [they bought a house while breaking this law - they loose the house].

Any industry handling other information, such as credit cards, MUST have a minimum set of security in place to do business. [Remember the TJ Maxx ID theft?] Example - every retail store must use the latest security, and it must be up to the credit card companies they deal with to enforce that security, under direct control of the government, and under penalty of mandatory jail time for infractions. i.e. Macy's accepts VISA, and sends information by wired and wireless nodes to process the transaction. VISA would be REQUIRED to CHECK the Macy's setup, and it MUST PASS the GOVERNMENTS rules, or they are not allowed to do business with Macy's. Further, if they do accept charges on a system that is not up to code would be a mandatory sentence for the CEO, Vp of Sales, and any other "chain of command" position in VISA would face at least 30 days behind bars. This is THE ONLY WAY to get complete compliance - no more "we will or have fixed the problem, but neither take or admit

No. of Copies rec'd 0+4
 List ABCDE

9/3/2009

responsibility for any wrongdoing".

Timeframes for security upgrades of any system, new or 'in place', should be very short [1-3 months at most], but also the "bugs" in the systems should be well thought out so that there will not be changes more than once per year to keep costs low. While businesses will cry about having to add equipment, spend money, etc., they really have NO RIGHT to NOT do the things necessary to protect personal information. It is OUR information and WE DO HAVE A RIGHT to have it protected.

These restrictions, and laws, should be enacted because it is not simply "a financial transaction" they are handling, but the very lives of the people of this country. Lives are ruined by ID theft every day, and we are talking about putting "lives" online - you should be doing everything possible to make that theft IMPOSSIBLE.

Charles H Miller II
2905 Rosemeade Dr
Fayetteville, NC 28306