

January 4, 2007

To Whom It May Concern,

My name is [redacted]. I'm a business owner (an advertising and marketing firm) in Austin, Texas. I can be reached via my cell phone at [redacted].

First, I wish to voice my support for the Identity Theft Task Force's work. I have quickly reviewed your initial recommendations. And they all make sense.

Needless to say, we all are prospective "victims" of ID Theft. And, as it has been estimated that something approaching 100 million individuals' records (including personally identifiable information) have been compromised in recent years because of poor information security policies and practices, I know that each of you must feel a tremendous responsibility and sense of urgency in the Task Force's work.

I preface my remarks by saying that I am not a technology expert. And I am certainly not someone who is versed in the technical details of effective security countermeasures.

But, based on my extensive research, I have learned of the critically important work of the Trusted Computing Group (www.trustedcomputinggroup.org), an 140-member, open standards organization that, among its other activities, has enabled the creation of a "core root of trust" for PCs: the trusted platform module (or TPM) which has already shipped within something like 50 million PCs from such brand names as Dell, Gateway, IBM, Lenovo, Fujitsu, Motion Computing, and others.

If the Task Force is not aware of the Trusted Computing Group's (TCG) far-reaching work, I highly recommend that some kind of liaison activity be initiated.

While potential victims of phishing schemes and other ID Theft threats must take more responsibility for their own protection and learn all that they can about active scripting, "safe" surfing, and basic computer data hygiene, it is also critical, in my opinion, that there be TPMs in consumer PCs as soon as possible. Thus far, PC manufacturers have adopted TPMs almost exclusively for use in business systems. (Additionally, I should note that both the U.S. Army and Air Force have issued requirements that specify TPMs in all future PC acquisitions.) This is a good first step. After all, when TPMs are initialized and leveraged within enterprise networks, they offer strong, hardware-based protection against security threats.

However, the “Average Joe” is still only being offered PCs that do not have this “core root of trust.”

The TPM chip is a commodity item. It adds something like \$2 to the cost of a typical laptop or desktop machine. There is no reason why PC manufacturers have not seen fit to put TPMs in all consumer machines.

From my reading, I can say with complete certainty that IF all consumer PCs had TPMs (with supporting software available from various sources) to protect their personally identifiable information, that ID thieves would have a significant hurdle to overcome.

I urge the members of the Identity Theft Task Force to become familiar with the Trusted Computing Group’s work and investigate what kind of market or legislative incentives might encourage PC manufacturers to do what is in the public’s best interests, i.e. make certain that all PCs contain Trusted Platform Modules.

In closing, let me acknowledge the obvious. There is no “silver bullet” in security technology that will eliminate ID Theft. Technology is, as I have noted, only ONE facet of the solution. However, when a technology that has been built upon open, published standards offers such promise, it seems a waste for it not to be applied across the boards, protecting networks and preserving trust.

Best wishes,

[redacted]