

**1. Maintaining Security of Consumer Data**

- 1) No comment or recommendation – my experience is in the private sector.
- 2) There is really no need to analyze the extent of SSN use within the private sector – just to determine if it’s being used and how. SSN is being used and used extensively in everything from schools to veterinarian offices to county fairs. Doing a study to determine if it’s being used would be a huge waste of money. Any further study of this situation should be done only as an assist in determining best alternatives to use instead.
- 3) Imposing National Data Security Standards would be the absolute wrong way to go, regardless of whether or not the variables of economic sector, business model or business size are considered. Lack of resource to enforce these standards would be the main drawback. In addition, and probably most importantly, if all entities are forced to “do security” in a similar manner based on regulated standards, eventually a way to breach those standards will be available. Time, ingenuity, and resources will always win out as nothing is perfect in the security world.
- 4) Breach notifications MUST be uniform throughout the nation, and again enforcement is paramount to the success of this endeavor. This is not an area where economic sector, business model, or business size should require different responses. Any entity that breaches personal information should be required to notify when appropriate. Careful thought must be given to thresholds that trigger notifications, or public apathy toward these will set in quickly if people are “over-notified”. Ridiculous add-on language such as that which allows the entity experiencing a data breach to decide if any harm may come to individuals because of the breach, should NEVER be considered. Any time data has been breached, or has the potential to be used against an individual due to poor data protection habits of an organization, notification should occur. There also needs to be significant sanctions in place to ensure this occurs. Again, success of this initiative will depend heavily on the ability to provide resources to police this situation.
- 5) This area can’t be stressed highly enough. Overall awareness among entities and consumers alike needs to be raised as soon as possible. Essential campaign elements should be:
  - a. For entities –
    - i. need to provide details when asked of how data is used, and how long it’s kept.
    - ii. Need to be educated on possible sanctions they may face,
    - iii. Need to be aware of best practices to employ within their company including policies that are followed; employee training; monitoring; incident response plans; disaster recovery plans; etc.
  - b. For consumers –
    - i. Need to understand what info is the most important to protect (SSN, any and all account numbers, medical info, banking info, retirement info, kid’s info too, etc.)

- ii. Need to be made aware of their rights,
- iii. Need to understand they can't litigate every time a breach occurs,
- iv. Need to raise awareness of scams,
- v. Need to know what resources are available to them

## **2. Preventing the Misuse of Consumer Data**

Two major changes would go a long way toward eliminating most identity theft in today's world –

- 1) Allow consumers to “turn off” instant credit and have their information revealed only when they approve it. The current system of the 3 credit bureaus not allowing this unless you can prove you are the victim of identity theft is outrageously wrong. It's MY data, if I don't want it shared with anybody unless I say so, then I should have that right. To this day, I am completely frustrated as to why I can't get this done.
- 2) My data, held at a data broker should be available to me whenever I ask to see it. ALL of it, not just parts. If a third party is gathering information on me from a number of sources – many unreliable. I should at least be able to see what information is being shared with potential employers, insurance companies, et al. Again, it's MY data – I should be able to do with it what I want, and I find it alarming that companies like Choicepoint have so much say in how my life unfolds. Again, just ridiculous and needs to be corrected immediately.

As for the remaining sections, these are outside of my specialty. I support each item, and recognize that each is an important component to this situation, but I don't feel I can offer anything of value. On a personal note, I do find it frustrating that victims of identity theft struggle as much as they do to correct the situation. Certainly innocent until proven guilty is lost in the translation by most entities, so anything that can be done to alleviate this would be a step in the right direction.

One last comment, identity theft for financial gain has captured most of the attention in the media. An area that has not gotten as much publicity, but surely will, is identify theft for medical services. This has the potential to create literally lethal situations for consumers who are subject to this crime. Proactive approach to this is needed soon, or we will be passing legislation only after a number of people have died needlessly.