Public Entity Breach Recommendations:
Wm. Scott Wolford
November 16, 2016
Testimony to the Public Utilities and Technology Committee of the Utah State Legislature.

I appear only as a concerned citizen and not representing my employer or any other group.

In October 2015 I retired from the Utah National Guard having served twenty-four years in the reserve component of the U.S. Army. Less than a month after my retirement, I received a notice from the Office of Personnel Management that my data may have been compromised in a massive data breach. The roots of this breach began in November of 2013, with my information being breached around June of 2014 and discovered by OPM in April or May of 2015. Recognizing that individual notifications take time to organize and execute, perhaps the six or seven months is a reasonable amount of time, however, no notice was distributed through my unit via the Utah National Guard which was presumably aware of the breach and potential impact.

My personal information that could have been breached included:

- My Social Security Number
- My residency and educational history
- My employment history
- Information about immediate family - and personal and business acquaintances
- My Health and financial history
- My Fingerprints
- And a username and password used to access federal systems.

When I was notified about this breach, I was encouraged to change my username and password - noting that this was six months after OPM publicly disclosed the breach.

I learned later that in congressional testimony, the former OPM director confirmed that Social Security Numbers and other information was stored in an unencrypted state because of the antiquated technology the OPM relied upon.

I recognize the Utah Legislature has nothing to do with and cannot correct inadequate security measures and inadequate notifications made by our federal friends, however I believe we in Utah should be better. The appetite for personal constituent information in the public sector is voracious and I believe often outpaces our capacity to be responsible stewards of that data. I believe the failures of our federal counterparts serve as cautionary tales to ensure our own house is order. As citizens we voluntarily and often involuntarily provide information to public-sector entities. It is wholly appropriate that public entities are compelled to make responsible notifications when breaches occur.

I will reference the Utah Protection of Personal Information Act - Utah Code Title 13 Chapter 44.

This act came from SB69 in the 2006 General Session sponsored by Senator Carlene Walker with Representative David Clark serving as House sponsor. The original intent of the bill was to ensure Utahns whose data was compromised through a consumer credit database were notified of such a breach. I commend the sponsors of this bill: it filled a legal gap that existed at the time and also made a very clear definition of Personal Information that has held up quite well for a decade. (When this bill was passed, Pluto was still a planet, Facebook was an infant, and Internet Explorer was the browser of choice.)

13-44-201

(1)
(a) A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine ***the likelihood that personal information has been or will be misused for identity theft or fraud purposes.***
(b) If an investigation under Subsection (1)(a) reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.

I am troubled by the lens data stewards use to decide whether notice should be made to those whose information has been breached. Again - **the steward of the data determines: the likelihood that personal information has been or will be misused for identity theft or fraud purposes."**

- The intent of the hacker should be immaterial to the requirement of constituent notification.
    - If personal information defined in Section 102 has been breached, this should require an expeditious notification.
- Notifications to constituents whose data has been breached should be initiated as soon as the system is secure and doing so would not compromise the investigation.
    - There is a balance in valuing catching the bad guys and informing victims.
- Not all breaches are equal:
    - The classification of the data and size of the breach should trigger certain notification requirements
        - Larger breaches should require a public notice be made in addition to notifying victims individually.

- I question the placement of this act in Title 13 “Commerce and Trade.” In a non-scientific and very small sampled inquiry I doubt smaller public entities are aware of this requirement. I believe a question worth asking is whether public and private entities whose data are breached should be treated the same in statute. If a public-sector system user finds his or her password has been changed and s/he didn’t do it, do we take the next step to find if a system has been accessed following that change. Do we keep system logs of what was accessed during that time. Should this trigger an investigation, or does the user simply change his or her password again and hope everything is fine. Conducting in “good faith a reasonable and prompt investigation” leaves a fair amount of discretion within the entity if individual system users are untrained on cyber security incident plans or such plans do not exist.

I appreciate the time from this committee and would be willing to attempt to answer any questions you would have.