

HB 2721 Feedback from the International Association for Human Resource Information Management Privacy and Security Special Interest Group Board of Directors

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (i) social security number; (ii) Virginia driver's license number; or, (iii) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. For purposes of this chapter, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Summary Commentary- If there is any encryption requirement it should be for the entire set of records since the additional encryption of name and SSN (as an example) is not any more burdensome and prevents overlapping breaches from more value to thieves.

The definition of what effective encryption is an open debate and difficult to define

. Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Summary Commentary- The idea of data ownership can be a difficult issue. The concept that each individual owns his or her own data may have some basis. The idea of data custodianship or data stewardship may be more appropriate. The EU model bases much of its practices upon this idea.

Notification to major statewide media.

Specific Comment- Having grown up in a very rural area – and having been to some very rural areas in Virginia. . . . there are places in Virginia where there are no “major statewide media” outlets. Places

where there are no major VA-based radio stations that come in clearly, places where there are no major newspapers. How about something like: major statewide and regional media”?

Notwithstanding subsection E, an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security.

Summary Comments- What qualification beyond the agencies affirmation provides some kind of assurance the agencies notification procedures are effective and ready to be used?

If an agency, upon providing a disclosure pursuant to this section, indicates that the individual may obtain a copy of his credit report from a consumer-reporting agency, the agency shall consult the consumer reporting agency as to the timing, content and distribution of the disclosure

Summary Comments- The actual meaning of this paragraph was confusing to several reviewers. The specific meaning seems lost.

“Breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by that person.

Suggested change of “personal information maintained by that person.” , to read, “personal information associated with that person.”

shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of the Commonwealth whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided

Specific Commentary- It seems to me that, the following scenario would require disclosure. . . . Jim mails a listing of his direct reports (including SSN) back to John Smith, his HR rep, through the inter-

office mail. The mail person makes a mistake and delivers it to John Smith who works in the cafeteria. John opens it – realizes that it should go to the John in HR (because this sort of thing happens at least every month) and he walks it over to the “right” John Smith. No harm, no foul, no problem; no investigation needed. There are a thousand such scenarios. . . .

This scenario doesn't seem to fall within the “good faith acquisition” exclusion provided in Paragraph A.

Part of the problem is the term “any breach of the security of the system”. How about this: “any breach of the security of the system that could reasonably be considered to place the information at risk”.

F. Notwithstanding subsection E, a person that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this section, shall be deemed to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Specific Commentary- Needs to be some requirement that those notification procedures are reviewed periodically and are reasonable