Synopsis of Senate Committee Amendments[*]

Dennis M. Papp *Legislative Service Commission*

Sub. H.B. 104

126th General Assembly
(S. Judiciary on Criminal Justice)

Expanded the provision of the House-passed version of the bill that requires state agencies to provide notice, in specified circumstances, of a breach of the security of a computerized data system, so that it also applies to agencies of a political subdivision.

Revised the provision of the House-passed version of the bill that required persons and "businesses" to provide notice, in specified circumstances, of a breach of the security of a computerized data system, so that it applies to businesses only if they are business entities that conduct business in Ohio; related to this, defines "business entity," includes "business entities" within the definition of "person," and makes the provision apply to "persons."

Revised the circumstances in which a state agency or person (or an agency of a political subdivision as amended by the Committee) must provide notice of a breach of the security of a computerized data system, so that an agency or person that owns or licenses computerized data that includes personal information must disclose a breach of the security of a computerized data system to any Ohio resident whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

Revised the circumstances in which a state agency or person (or an agency of a political subdivision as amended by the Committee) must notify another agency or person of a breach of the security of a computerized data system, so that an agency or person that, on behalf of or at the direction of another agency or person, is the custodian of or stores computerized data that includes personal information must notify the other agency or person of a breach of the security of the system if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person

[*] This synopsis does not address amendments that may have been adopted on the Senate floor.

and if the access and acquisition causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

Revised the definitions of "breach of the security of a computerized data system," "personal information," and "system" that apply regarding the duties described in the preceding two paragraphs; related to the definition of "personal information," defined the terms "encryption" and "redaction" and clarified what is meant be an alteration; replaced the definition of the term "business" with a definition of the term "business entity."

Clarifies that the determination of when the notice must be provided must include time to determine which residents' personal information was accessed and acquired.

Expanded the circumstances in which a state agency or person (or an agency of a political subdivision as amended by the Committee) may delay a disclosure to include circumstances in which a law enforcement agency determines that disclosure or notification will jeopardize homeland or national security.

Revised the manners in which a state agency or person (or an agency of a political subdivision as amended by the Committee) generally must make a required disclosure or notification, and added two sets of circumstances in which an agency or person may provide substitute notice in separate, specified manners other than a standard notice (the circumstances are: (1) if the agency or person does not have sufficient information to provide a standard notice, if the cost of a standard notice would exceed $250,000, or if the affected class of subject residents to whom notice must be provided exceeds 500,000 persons, or (2) if the agency or person has 10 employees or fewer and the cost of providing the notice to residents to whom notice must be provided will exceed $10,000).

Removed the provision of the House-passed version of the bill that would have permitted an agency or person that maintains its own disclosure or notification procedures as part of an information privacy or security policy for the treatment of personal information to satisfy the bill's notification requirements by using those procedures, if the procedures were consistent with the bill's timing requirements.

Provided that, if a state agency or person (or an agency of a political subdivision as amended by the Committee) provides notice to a consumer reporting agency under a retained provision of the House-passed version of the bill, in no case may the agency or person delay any other disclosure or notification required under the bill in order to make the notification to the consumer reporting agency.

Provided that the Attorney General has the exclusive authority to bring a civil action to enforce the disclosure and notification provisions of the bill.

Revised the civil penalty to be assessed by a court in a civil action brought as described in the preceding paragraph, if it determines that a state agency or person (or an agency of a political subdivision as amended by the Committee) intentionally or recklessly failed to comply with a disclosure or notification requirement under the bill, so

that the civil penalty is as follows: (1) up to $1,000 for each of the first 60 days that the agency or person failed to comply, (2) up to $5,000 for each day commencing on the 61st day through the 90th day that the agency or person failed to comply, and (3) up to $10,000 for each day commencing on the 91st day and continuing thereafter that the agency failed to comply.

Required the court, in determining the appropriate civil penalty to assess as described in the preceding paragraph, to consider all relevant factors, including whether or not there was bad faith involved in the failure to comply.

H0104-126.doc/ss 10/25/05