Dennis M. Papp *Legislative Service Commission*

Sub. H.B. 104*

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

Reps. Martin, McGregor, Trakas, Wagoner, C. Evans, Perry, Seitz, Coley, Core, Harwood, Allen, Beatty, Blessing, Bubp, Buehrer, Carano, Cassell, Collier, DeBose, DeGeeter, Distel, Dolan, Domenick, Faber, Fende, Fessler, Flowers, Gibbs, Gilb, Hughes, Kearns, Latta, Mason, Miller, Oelslager, Otterman, S. Patton, T. Patton, Raussen, Reidelbach, Reinhard, Sayre, Schaffer, Schneider, Seaver, Setzer, Skindell, G. Smith, S. Smith, D. Stewart, J. Stewart, Strahorn, Williams

BILL SUMMARY

- Requires any state agency or agency of a political subdivision that owns or licenses computerized data that includes personal information of a specified nature to disclose, in the most expedient time possible but generally not later than 45 days following its discovery or notification of the security breach, any breach of the security of the 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 by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

- Requires any state agency or agency of a political subdivision that, on behalf of or at the direction of another state agency or agency of a political subdivision, is the custodian of or stores computerized data that includes personal information of a specified nature to notify that other state agency or agency of a political subdivision of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by

* *This analysis was prepared before the report of the Senate Judiciary on Criminal Justice Committee appeared in the Senate Journal. Note that the list of co-sponsors and the legislative history may be incomplete.*

the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of Ohio.

- Requires any person (which is defined as including any business entity that conducts business in Ohio) and that owns or licenses computerized data that includes personal information of a specified nature to disclose, in the most expedient time possible but generally not later than 45 days following its discovery or notification of the security breach, any breach of the security of the 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 by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

- Requires any person that on behalf of or at the direction of another person or a governmental entity is the custodian of or stores computerized data that includes personal information of a specified nature to notify that other person or governmental entity of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of Ohio.

- Permits a state agency, agency of a political subdivision, or person, whichever is applicable, to delay the required disclosure or notification if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security.

- Specifies the methods by which a state agency, agency of a political subdivision, or person may disclose or make a notification as required by the bill.

- Requires a state agency, agency of a political subdivision, or person, whichever is applicable, that discovers circumstances requiring disclosure to more than 1,000 Ohio residents involved in a single occurrence of a breach of the security of the system to notify without unreasonable delay all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given to Ohio residents

pursuant to the bill; provides that, in no case may a state agency, agency of a political subdivision, or person delay any disclosure or notification required under the provisions described in the preceding dot points in order to make the notification to consumer reporting agencies.

- Provides that a financial institution, trust company, or credit union or affiliate of any of those entities that is required by federal law to notify its customers of an information security breach with respect to information about those customers and that is subject to its government regulatory agency's examination for compliance with that law is exempt from the bill's requirements with respect to disclosure by *any person*.

- Provides that the bill's provisions pertaining to the required disclosure and notification by *any person* do not apply to any person or entity regulated by the Health Insurance Portability and Accountability Act (HIPAA).

- Provides that any waiver of the bill's provisions pertaining to the required disclosure and notification by *any person* is contrary to public policy and is void and unenforceable.

- Authorizes the Attorney General to conduct an investigation and grants the Attorney General subpoena authority if the Attorney General has reason to believe that a state agency, agency of a political subdivision, or person has failed or is failing to comply with the bill's requirements, and prescribes procedures upon issuance of a subpoena by a court.

- Grants the Attorney General the exclusive authority to bring a civil action in a court of common pleas if it appears that a state agency, agency of a political subdivision, or person has failed or is failing to comply with the bill's requirements and requires the court, upon a finding of such failure, to impose a civil penalty of a specified amount per day for each day the state agency, agency of a political subdivision, or person fails to comply with the bill (briefly, the civil penalty is up to $1,000 for the first 60 days, up to $5,000 for the 61st day through the 90th day, and up to $10,000 for the 91st day and succeeding days that the agency or person has intentionally or recklessly failed to comply with the applicable requirement under the bill).

- Provides that any civil penalty assessed as described in the preceding dot point must be deposited into the Consumer Protection Enforcement Fund

for the sole purpose of paying expenses incurred by the Consumer Protection Section of the Attorney General's Office.

- Specifies that, in determining the appropriate civil penalty to assess as described in the second preceding dot point, the court must consider all relevant factors, including: (1) if the defendant in the civil action is a state agency, an agency of a political subdivision, or a person that is a business entity, whether or not the high managerial officer, agent, or employee of the agency or business entity having supervisory responsibility for compliance with the bill's applicable disclosure requirements acted in bad faith in failing to comply with them, and (2) if the defendant in the civil action is a person other than a business entity, whether or not the person acted in bad faith in failing to comply with the bill's disclosure requirements applicable to persons.

- States that it deals with a matter of statewide concern and that the General Assembly intends that the bill supersede and preempt all local rules, regulations, resolutions, codes, and ordinances that pertain to matters expressly set forth or regulated under the bill.

TABLE OF CONTENTS

CONTENT AND OPERATION

Disclosure or notification by state agency or agency of a political subdivision of breach of security of personal information system

The bill generally provides for a state agency's or agency of a political subdivision's disclosure to Ohio residents of any breach of security of the agency's computerized data that includes personal information about the residents, if an unauthorized person accessed and acquired the personal information and it causes or reasonably is believed will cause a material risk of identity theft or other fraud to the residents, or notification of any such breach of security to another state agency or political subdivision agency on behalf of which computerized data that includes personal information is in the custody of or stored by the agency.

Requirement for disclosure or notification

The bill requires any "state agency" or "agency of a political subdivision" that owns or licenses computerized data that includes "personal information" to disclose any "breach of the security of the system," following its discovery or notification of the breach of the security of the system, to any resident of Ohio whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. (See "***Definitions for purposes of disclosure or notification by state agency or political subdivision agency***," below, for definitions of the terms in quotation marks.) The disclosure may be made pursuant to any provision of a contract entered into by the agency with any person or another agency prior to the date the breach of the security of the system occurred if that contract does not conflict with any provision of the bill regarding state agency or political subdivision agency disclosure. For the purposes of this provision, a resident of Ohio is an individual whose principal mailing address as reflected in the records of the state or political subdivision agency is in Ohio. The state or political subdivision agency must make that disclosure in the most expedient time possible but not later than 45 days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described below and consistent with any measures necessary to determine the scope of the breach, including which

residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system. (R.C. 1347.12(B).)

The bill also requires any state agency or political subdivision agency that, on behalf of or at the direction of another state agency or political subdivision agency, is the custodian of or stores computerized data that includes personal information to notify that other agency of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of Ohio (R.C. 1347.12(C)).

The bill permits the agency to delay the required disclosure or notification described in the two preceding paragraphs and the notification described below in "***Disclosure or notification of breach of security of system involving more than 1,000 persons; consumer reporting agencies***," if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the agency must make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security (R.C. 1347.12(D)).

Methods of disclosure or notification

The bill provides that a state agency or political subdivision agency may disclose or make a notification as described above by any of following methods (R.C. 1347.12(E)):

(1) Written notice;

(2) Electronic notice, if the agency's primary method of communication with the resident to whom the disclosure must be made is by electronic means;

(3) Telephone notice;

(4) Substitute notice in accordance with this paragraph if the agency required to disclose demonstrates that the agency does not have sufficient contact information to provide notice in a manner described in (1), (2), or (3), above, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed $250,000, or that the affected class of subject residents to whom disclosure or notification is required exceeds 500,000 persons. Substitute notice under this provision must consist of all of the following: (a) electronic mail notice if the agency has an electronic mail address

for the resident to whom the disclosure must be made, (b) conspicuous posting of the disclosure or notice on the agency's web site, if the agency maintains one, and (c) notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds 75% of Ohio's population.

(5) Substitute notice in accordance with this paragraph, if the agency required to disclose demonstrates that the agency has 10 employees or fewer and that the cost of providing the disclosures or notices to residents to whom disclosure or notification is required will exceed $10,000. Substitute notice under this provision must consist of all of the following: (a) notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the agency is located, which advertisement must be of sufficient size that it covers at least 1/4 of a page in the newspaper and must be published in the newspaper at least once a week for three consecutive weeks, (b) conspicuous posting of the disclosure or notice on the agency's web site, if the agency maintains one, and (c) notification to major media outlets in the geographic area in which the agency is located.

Disclosure or notification of breach of security of system involving more than 1,000 persons: consumer reporting agencies

The bill provides that, if a state agency or political subdivision agency discovers circumstances that require disclosure to more than 1,000 Ohio residents involved in a single occurrence of a breach of the security of the system, the agency must notify, without unreasonable delay, all "consumer reporting agencies that compile and maintain files on consumers on a nationwide basis" (see "***Definitions for purposes of disclosure or notification by state agency or political subdivision agency***," below) of the timing, distribution, and content of the disclosure given by the agency to the Ohio residents. In no case may a state agency or political subdivision agency delay any disclosure or notification required under the provisions described above in "***Requirement for disclosure or notification***" in order to make the notification to consumer reporting agencies. (R.C. 1347.12(F).)

Definitions for purposes of disclosure or notification by state agency or agency of a political subdivision

The bill defines the following terms for purposes of its provisions requiring a state agency or political subdivision agency to make the disclosure or notification described above (R.C. 1347.12(A)):

"***State agency***" means every organized body, office, or agency established by the laws of Ohio for the exercise of any function of state government (by reference to existing R.C. 1.60, not in the bill).

"***Agency of a political subdivision***" means each organized body, office, or agency established by a political subdivision for the exercise of any function of the political subdivision. "Political subdivision" has the same meaning as in the Political Subdivision Sovereign Immunity Law contained in R.C. Chapter 2744. (R.C. 1347.12(A)(1).)

"***Personal information***" means an "individual's" (defined as a natural person) name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: (1) Social Security number, (2) driver's license number or state identification card number, or (3) account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account. "Personal information" does *not* include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed: (1) any news, editorial, or advertising statement published in any *bona fide* newspaper, journal, or magazine, or broadcast over radio or television, (2) any gathering or furnishing of information or news by any *bona fide* reporter, correspondent, or news bureau to news media described in clause (1) of this sentence, (3) any publication designed for and distributed to members of any *bona fide* association or charitable or fraternal nonprofit corporation, or (4) any type of media similar in nature to any item, entity, or activity identified in clause (1), (2), or (3) of this sentence.

"***Breach of the security of the system***" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a state agency or an agency of a political subdivision and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of Ohio. Good faith acquisition of personal information by an employee or agent of the state agency or agency of the political subdivision for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory state agency, is not a breach of the security of the system.

"***Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis***" means a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's creditworthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide: (1) public record information, and (2) credit account information from persons who furnish that information regularly and in the ordinary course of business.

"***Encryption***" means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

"***Record***" means any information that is stored in an electronic medium and is retrievable in perceivable form. "Record" does *not* include any publicly available directory containing information an individual voluntarily has consented to have publicly disseminated or listed, such as name, address, or telephone number.

"***Redacted***" means altered or truncated so that no more than the last four digits of a Social Security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data.

"***System***" means any collection or group of related records that are kept in an organized manner, that are maintained by a state agency or agency of a political subdivision, and from which personal information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. "System" does not include any collected archival records in the custody of or administered under the authority of the Ohio Historical Society, any published directory, any reference material or newsletter, or any routine information that is maintained for the purpose of internal office administration of the agency, if its use would not adversely affect an individual, and if there has been no unauthorized external breach of the directory, material, newsletter, or information.

Disclosure or notification by any person of breach of security of personal information system

The bill generally provides for the disclosure by any person, including a business entity conducting business in Ohio, to residents of Ohio of any breach of security of computerized data that includes personal information about the residents, if an unauthorized person accessed and acquired the personal information and it causes or reasonably is believed will cause a material risk of

identity theft or other fraud to the residents, or notification of any such breach of security to another person or a governmental entity on behalf of which computerized data that includes personal information is in the custody of or stored by the person.

Requirement for disclosure or notification

The bill requires any "person" (including a business entity that conducts business in Ohio; for purposes of the remaining portions of this part of this analysis, references to "person" include such a business entity) and that owns or licenses computerized data that includes "personal information" to disclose any "breach of the security of the system," following its discovery or notification of the breach of the security of the system, to any resident of Ohio whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident. (See "***Definitions for purposes of disclosure or notification by any person***," below, for definitions of the terms in quotation marks.) The disclosure may be made pursuant to any provision of a contract entered into by the person with another person prior to the date the breach of the security of the system occurred if that contract does not conflict with or waive any provision of the bill regarding disclosure by a person. For the purposes of this provision, a resident of Ohio is an individual whose principal mailing address as reflected in the records of the person or business is in Ohio. The person must make the required disclosure in the most expedient time possible but not later than 45 days following its discovery or notification of the breach in the security of the system, subject to the legitimate needs of law enforcement activities described below and consistent with any measures necessary to determine the scope of the breach, including which residents' personal information was accessed and acquired, and to restore the reasonable integrity of the data system. (R.C. 1349.19(B).)

The bill also requires any person that on behalf of or at the direction of another person or on behalf of or at the direction of a governmental entity, is the custodian of or stores computerized data that includes personal information to notify that other person or governmental entity of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of Ohio (R.C. 1349.19(C)).

A person may delay the required disclosure or notification as described in the two preceding paragraphs and the notification described below in "***Disclosure or notification of breach of security of system involving more than 1,000***

persons; consumer reporting agencies," if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security, in which case, the person must make the disclosure or notification after the law enforcement agency determines that disclosure or notification will not compromise the investigation or jeopardize homeland or national security (R.C. 1349.19(D)).

Methods of disclosure or notification

A person may disclose or make a notification as described above by any of the following methods (R.C. 1349.19(E)):

(1) Written notice;

(2) Electronic notice, if the person's primary method of communication with the resident to whom the disclosure must be made is by electronic means;

(3) Telephone notice;

(4) Substitute notice in accordance with this paragraph, if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described in (1), (2), or (3), above, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed $250,000, or that the affected class of subject residents to whom disclosure or notification is required exceeds 500,000 persons. Substitute notice under this provision must consist of all of the following: (a) electronic mail notice if the person has an electronic mail address for the resident to whom the disclosure must be made, (b) conspicuous posting of the disclosure or notice on the person's web site, if the person maintains one, and (c) notification to major media outlets, to the extent that the cumulative total of the readership, viewing audience, or listening audience of all of the outlets so notified equals or exceeds 75% of Ohio's population.

(5) Substitute notice in accordance with this paragraph, if the person required to disclose demonstrates that the person is a business entity with 10 employees or fewer and that the cost of providing the disclosures or notices to residents to whom disclosure or notification is required will exceed $10,000. Substitute notice under this provision must consist of all of the following: (a) notification by a paid advertisement in a local newspaper that is distributed in the geographic area in which the business entity is located, which advertisement must be of sufficient size that it covers at least 1/4 of a page in the newspaper and must be published in the newspaper at least once a week for three consecutive weeks, (b) conspicuous posting of the disclosure or notice on the business entity's web

site, if the entity maintains one, and (c) notification to major media outlets in the geographic area in which the business entity is located.

Exemption for certain financial institutions, trust companies, credit unions, and affiliates that are subject to a federal notification requirement

The bill provides that a financial institution, trust company, or credit union or any affiliate of a financial institution, trust company, or credit union that is required by federal law, including, but not limited to, any federal statute, regulation, regulatory guidance, or other regulatory action, to notify its customers of an information security breach with respect to information about those customers and that is subject to examination by its functional government regulatory agency for compliance with the applicable federal law, is exempt from the bill's requirements regarding disclosure by a person (R.C. 1349.19(F)(1)).

Disclosure or notification of breach of security of system involving more than 1,000 persons: consumer reporting agencies

If a person discovers circumstances that require disclosure to more than 1,000 Ohio residents involved in a single occurrence of a breach of the security of the system, the person must notify, without unreasonable delay, all "consumer reporting agencies that compile and maintain files on consumers on a nationwide basis" (see "***Definitions for purposes of disclosure or notification by any person or business***," below) of the timing, distribution, and content of the disclosure given by the person to the Ohio residents. In no case may a person delay any disclosure or notification required under the provisions described above in "***Requirement for disclosure or notification***" in order to make the notification to consumer reporting agencies. (R.C. 1349.19(G).)

Nonwaivable duties

Any waiver of the above provisions requiring disclosure or notification by a person is contrary to public policy and is void and unenforceable (R.C. 1349.19(H)).

Application of bill

The above provisions regarding disclosure by a person do not apply to any person or entity regulated by sections 1171 to 1179 of the Social Security Act (Health Insurance Portability and Accountability Act or HIPAA) and any corresponding regulations (R.C. 1349.19(F)(2)).

Definitions for purposes of disclosure or notification by any person or business

The bill defines the following terms for purposes of its provisions requiring any person to make the above described disclosure or notification (R.C. 1349.19(A)):

"***Person***" has the same meaning as in existing R.C. 1.59, not in the bill, except that "***person***" includes a business entity (see below) only if the business entity conducts business in Ohio.

"***Business entity***" means a sole proprietorship, partnership, corporation, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of Ohio, any other state, the United States, or any other country, or the parent or subsidiary of a financial institution.

"***Personal information***," "***Consumer reporting agency that compiles and maintains files on consumers on a nationwide basis***," "***Record***," "***Encryption***," and "***Redacted***" are defined in the same manner as described above in "***Definitions for purposes of disclosure or notification by state agency or agency of a political subdivision***."

"***Breach of the security of the system***" means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of Ohio. Good faith acquisition of personal information by an employee or agent of the person for the purposes of the person is not a breach of the security of the system, provided that the personal information is not used for an unlawful purpose or subject to further unauthorized disclosure. Acquisition of personal information pursuant to a search warrant, subpoena, or other court order, or pursuant to a subpoena, order, or duty of a regulatory agency is not a breach of the security of the system.

"***System***" means any collection or group of related records that are kept in an organized manner, that are maintained by a person, and from which personal information is retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual. "System" does not include any published directory, any reference material or newsletter, or any routine information that is maintained for the purpose of internal office administration of the person, if its use would not adversely affect an individual, and if there has been no unauthorized external breach of the directory, material, newsletter, or information.

Investigation and enforcement by Attorney General

Investigation

The bill authorizes the Attorney General (AG) to conduct an investigation if the AG, based on complaints or the AG's own inquiries, has reason to believe that a state agency, agency of a political subdivision, or person has failed or is failing to comply with the respective disclosure requirements of the bill, as described above. In any such investigation, the AG may administer oaths, subpoena witnesses, adduce evidence, and subpoena the production of any book, document, record, or other relevant matter. If the AG subpoenas the production of any relevant matter that is located outside Ohio, the AG may designate a representative, including an official of the state in which that matter is located, to inspect the matter on the AG's behalf. The AG may carry out similar requests received from officials of other states. Any person who is subpoenaed to produce relevant matter must make that matter available at a convenient location in Ohio or the state of the representative designated as described above. (R.C. 1349.191(B), (C), and (D), 1347.12(G), and 1349.19(I).)

Court procedure upon subpoena

Any person who is subpoenaed as a witness or to produce relevant matter may file in the Court of Common Pleas of Franklin County, the county in Ohio in which the person resides, or the county in Ohio in which the person's principal place of business is located a petition to extend for good cause shown the date on which the subpoena is to be returned or to modify or quash for good cause shown that subpoena. The person may file the petition at any time prior to the date specified for the return of the subpoena or within 20 days after the service of the subpoena, whichever is earlier. Any person who is subpoenaed as a witness or to produce relevant matter under the provisions described in the preceding paragraph must comply with the terms of the subpoena unless the court orders otherwise prior to the date specified for the return of the subpoena or, if applicable, that date as extended. If a person fails without lawful excuse to obey a subpoena, the AG may apply to the court of common pleas for an order that does one or more of the following: (1) compels the requested discovery, (2) adjudges the person in contempt of court, (3) grants injunctive relief to restrain the person from failing to comply with the applicable disclosure requirements, (4) grants injunctive relief to preserve or restore the status quo, or (5) grants other relief that may be required until the person obeys the subpoena. The court must impose a civil penalty on any person who violates a court order issued as described above. The civil penalty is to be imposed in the same manner as the imposition of a civil penalty in a civil action for a failure to comply with the disclosure requirements of the bill, as described above (see "***Civil action***," below). (R.C. 1349.191(E), (F), and (G) and 1349.192(A).)

Civil action

The bill grants the AG the exclusive authority to bring a civil action in a court of common pleas for appropriate relief, including a temporary restraining order, preliminary or permanent injunction, and civil penalties, if it appears that a state agency, agency of a political subdivision, or person has failed or is failing to comply with the respective disclosure requirements of the bill. Upon its finding of such a failure to comply, the court must impose a civil penalty upon the state agency, agency of a political subdivision, or person as follows: (1) for each day that the agency or person has intentionally or recklessly failed to comply with the applicable requirement, subject to clauses (2) and (3) of this sentence, a civil penalty of up to $1,000 for each day the agency or person fails to comply with the requirement, (2) if the agency or person has intentionally or recklessly failed to comply with the applicable requirement for more than 60 days, subject to clause (3) of this sentence, a civil penalty in the amount specified in clause (1) of this sentence for each day of the first 60 days that the agency or person fails to comply with the requirement and, for each day commencing with the 61st day that the agency or person has failed to comply with the requirement, a civil penalty of up to $5,000 for each such day the agency or person fails to comply with the requirement, (3) if the agency or person has intentionally or recklessly failed to comply with the applicable requirement for more than 90 days, a civil penalty in the amount specified in clause (1) of this sentence section for each day of the first 60 days that the agency or person fails to comply with the requirement, a civil penalty of up to $5,000 for each day commencing with the 61st day and continuing through the 90th day that the agency or person fails to comply with the requirement, and, for each day commencing with the 91st day that the agency or person has failed to comply with the requirement, a civil penalty of up to $10,000 for each such day the agency or person fails to comply with the requirement. Any civil penalty assessed under this provision must be deposited into the Consumer Protection Enforcement Fund to be used for the sole purpose of paying expenses incurred by the Consumer Protection Section of the AG's Office. (R.C. 1349.192(A)(1) and (2), 1347.12(G), 1349.19(I), and 1345.51.)

In determining the appropriate civil penalty to assess under the provisions described in the preceding paragraph, the court must consider all relevant factors, including the following: (1) if the defendant in the civil action is a state agency, an agency of a political subdivision, or a person that is a business entity, whether or not the high managerial officer, agent, or employee of the agency or business entity having supervisory responsibility for compliance with the applicable disclosure requirements of the bill, as described above, acted in bad faith in failing to comply with the requirements, and (2) if the defendant in the civil action is a person other than a business entity, whether or not the person acted in bad faith in

failing to comply with the disclosure requirements of the bill applicable to persons, as described above (R.C. 1349.192(A)(3)).

Any state agency, agency of a political subdivision, or person that is found by the court to have failed to comply with the applicable disclosure requirements in the bill is liable to the AG for the costs in conducting an investigation and bringing an action under the bill (R.C. 1349.192(B)).

The above rights and remedies are in addition to any other rights and remedies that are provided by law (R.C. 1349.192(C)).

Statewide concern--preemption

The bill states that it deals with a subject matter of statewide concern. It also states that it is the intent of the General Assembly that the bill supersede and preempt all rules, regulations, resolutions, codes, and ordinances of all counties, municipal corporations, townships, and agencies of counties, municipal corporations, and townships that pertain to matters that are expressly set forth or regulated under the bill. (Section 3.)

HISTORY

ACTION	DATE	JOURNAL ENTRY
Introduced	03-01-05	p. 240
Reported, H. Civil & Commercial Law	06-23-05	p. 1423
Passed House (90-0)	08-02-05	pp. 1587-1588
Reported, S. Judiciary on Criminal Justice	---	---

H0104-RS-126.doc/jc