

Ohio Revised Code

Title 13 – Commercial Transactions

Chapter 1349 – Consumer Protection

§ 1349.19 Private disclosure of security breach of computerized personal information data.

(A) As used in this section:

(1) (a) “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 this state.

(b) For purposes of division (A)(1)(a) of this section:

(i) 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.

(ii) 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.

(2) “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 this state, any other state, the United States, or any other country, or the parent or subsidiary of a financial institution.

(3) “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:

(a) Public record information;

(b) Credit account information from persons who furnish that information regularly and in the ordinary course of business.

(4) “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.

(5) “Individual” means a natural person.

(6) “Person” has the same meaning as in section 1.59 of the Revised Code, except that “person” includes a business entity only if the business entity conducts business in this state.

(7) (a) “Personal information” means an individual’s 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:

(i) Social security number;

(ii) Driver’s license number or state identification card number;

(iii) 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.

(b) “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:

(i) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television;

(ii) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media described in division (A)(7)(b)(i) of this section;

(iii) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation;

(iv) Any type of media similar in nature to any item, entity, or activity identified in division (A)(7)(b)(i), (ii), or (iii) of this section.

- (8) “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.
- (9) “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.
- (10) “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 the use of the directory, material, newsletter, or information would not adversely affect an individual, and there has been no unauthorized external breach of the directory, material, newsletter, or information.
- (B) (1) Any person that owns or licenses computerized data that includes personal information shall 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 this state 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. The disclosure described in this division 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 any provision of this section and does not waive any provision of this section. For purposes of this section, a resident of this state is an individual whose principal mailing address as reflected in the records of the person is in this state.
- (2) The person shall make the disclosure described in division (B)(1) of this section in the most expedient time possible but not later than forty-five 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 in division (D) of this section 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.
- (C) Any person that, on behalf of or at the direction of another person or on behalf of or at the direction of any governmental entity, is the custodian of or stores computerized data that includes personal information shall 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 this state.

(D) The person may delay the disclosure or notification required by division (B), (C), or (G) of this section 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 shall 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.

(E) For purposes of this section, a person may disclose or make a notification by any of the following methods:

(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 division, if the person required to disclose demonstrates that the person does not have sufficient contact information to provide notice in a manner described in division (E)(1), (2), or (3) of this section, or that the cost of providing disclosure or notice to residents to whom disclosure or notification is required would exceed two hundred fifty thousand dollars, or that the affected class of subject residents to whom disclosure or notification is required exceeds five hundred thousand persons. Substitute notice under this division shall 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;

(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 seventy-five per cent of the population of this state.

(5) Substitute notice in accordance with this division, if the person required to disclose demonstrates that the person is a business entity with ten employees or fewer and that the cost of providing the disclosures or notices to residents to

whom disclosure or notification is required will exceed ten thousand dollars. Substitute notice under this division shall 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 shall be of sufficient size that it covers at least one-quarter of a page in the newspaper and shall 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;

(c) Notification to major media outlets in the geographic area in which the business entity is located.

(F) (1) 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 requirements of this section.

(2) This section does not apply to any person or entity that is a covered entity as defined in 45 C.F.R. 160.103, as amended.

(G) If a person discovers circumstances that require disclosure under this section to more than one thousand residents of this state involved in a single occurrence of a breach of the security of the system, the person shall 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 by the person to the residents of this state. In no case shall a person that is required to make a notification required by this division delay any disclosure or notification required by division (B) or (C) of this section in order to make the notification required by this division.

(H) Any waiver of this section is contrary to public policy and is void and unenforceable.

(I) The attorney general may conduct pursuant to sections 1349.191 and 1349.192 of the Revised Code an investigation and bring a civil action upon an alleged failure by a person to comply with the requirements of this section.

§ 1349.191 Investigation of noncompliance with disclosure laws.

(A) As used in this section and section 1349.192 of the Revised Code:

(1) "Agency of a political subdivision" has the same meaning as in section 1347.12 of the Revised Code.

(2) “Business” has the same meaning as in section 1349.19 of the Revised Code.

(3) “State agency” has the same meaning as in section 1.60 of the Revised Code.

(B) The attorney general may conduct an investigation if the attorney general, based on complaints or the attorney general’s own inquiries, has reason to believe that a state agency or an agency of a political subdivision has failed or is failing to comply with section 1347.12 of the Revised Code or that a person has failed or is failing to comply with section 1349.19 of the Revised Code.

(C) In any investigation conducted pursuant to this section, the attorney general may administer oaths, subpoena witnesses, adduce evidence, and subpoena the production of any book, document, record, or other relevant matter.

(D) (1) If the attorney general under division (C) of this section subpoenas the production of any relevant matter that is located outside this state, the attorney general may designate a representative, including an official of the state in which that relevant matter is located, to inspect the relevant matter on the attorney general’s behalf. The attorney general may carry out similar requests received from officials of other states.

(2) Any person who is subpoenaed to produce relevant matter pursuant to division (C) of this section shall make that relevant matter available at a convenient location within this state or the state of the representative designated under division (D)(1) of this section.

(E) Any person who is subpoenaed as a witness or to produce relevant matter pursuant to division (C) of this section may file in the court of common pleas of Franklin county, the county in this state in which the person resides, or the county in this state 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 twenty days after the service of the subpoena, whichever is earlier.

(F) Any person who is subpoenaed as a witness or to produce relevant matter pursuant to division (C) of this section shall 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 attorney general 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 section 1347.12 or 1349.19 of the Revised Code, whichever is applicable;

(4) Grants injunctive relief to preserve or restore the status quo;

(5) Grants other relief that may be required until the person obeys the subpoena.

(G) The court shall impose a civil penalty on any person who violates an order of a court issued under division (F) of this section in the same manner as the imposition of a civil penalty under section 1349.192 of the Revised Code for a failure to comply with section 1347.12 or 1349.19 of the Revised Code, whichever is applicable.

§ 1349.192 Civil action by attorney general for violation of disclosure laws.

(A) (1) The attorney general shall have the exclusive authority to bring a civil action in a court of common pleas for appropriate relief under this section, including a temporary restraining order, preliminary or permanent injunction, and civil penalties, if it appears that a state agency or an agency of a political subdivision has failed or is failing to comply with section 1347.12 of the Revised Code or that a person has failed or is failing to comply with section 1349.19 of the Revised Code. Upon its finding that a state agency or an agency of a political subdivision has failed to comply with section 1347.12 of the Revised Code or that a person has failed to comply with section 1349.19 of the Revised Code, the court shall impose a civil penalty upon the state agency, agency of a political subdivision, or person as follows:

(a) For each day that the state agency, agency of a political subdivision, or person has intentionally or recklessly failed to comply with the applicable section, subject to divisions (A)(1)(b) and (c) of this section, a civil penalty of up to one thousand dollars for each day the agency or person fails to comply with the section;

(b) If the state agency, agency of a political subdivision, or person has intentionally or recklessly failed to comply with the applicable section for more than sixty days, subject to division (A)(1)(c) of this section, a civil penalty in the amount specified in division (A)(1)(a) of this section for each day of the first sixty days that the agency or person fails to comply with the section and, for each day commencing with the sixty-first day that the state agency, agency of a political subdivision, or person has failed to comply with the section, a civil penalty of up to five thousand dollars for each such day the agency or person fails to comply with the section;

(c) If the state agency, agency of a political subdivision, or person has intentionally or recklessly failed to comply with the applicable section for more than ninety days, a civil penalty in the amount specified in division (A)(1)(a) of this section for each day of the first sixty days that the agency

or person fails to comply with the section, a civil penalty of up to five thousand dollars for each day commencing with the sixty-first day and continuing through the ninetieth day that the agency or person fails to comply with the section, and, for each day commencing with the ninety-first day that the state agency, agency of a political subdivision, or person has failed to comply with the section, a civil penalty of up to ten thousand dollars for each such day the agency or person fails to comply with the section.

(2) Any civil penalty that is assessed under division (A)(1) of this section shall be deposited into the consumer protection enforcement fund created by section 1345.51 of the Revised Code.

(3) In determining the appropriate civil penalty to assess under division (A)(1) of this section, the court shall consider all relevant factors, including the following:

(a) 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 section 1347.12 or 1349.19 of the Revised Code, whichever is applicable, acted in bad faith in failing to comply with the section.

(b) 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 section 1349.19 of the Revised Code.

(B) Any state agency or agency of a political subdivision that is found by the court to have failed to comply with section 1347.12 of the Revised Code or any person that is found by the court to have failed to comply with section 1349.19 of the Revised Code shall be liable to the attorney general for the attorney general's costs in conducting an investigation under section 1349.191 of the Revised Code and bringing an action under this section.

(C) The rights and remedies that are provided under this section are in addition to any other rights or remedies that are provided by law.