AN ACT relating to the security of personal information.

Be it enacted by the General Assembly of the Commonwealth of Kentucky:

➔Section 1. KRS 61.931 is amended to read as follows:

As used in KRS 61.931 to 61.934:

(1) "Agency" means:

(a) The executive branch of state government of the Commonwealth of Kentucky;

(b) Every county, city, municipal corporation, urban-county government, charter county government, consolidated local government, and unified local government;

(c) Every organizational unit, department, division, branch, section, unit, office, administrative body, program cabinet, bureau, board, commission, committee, subcommittee, ad hoc committee, council, authority, public agency, instrumentality, interagency body, special purpose governmental entity, or public corporation of an entity specified in paragraph (a) or (b) of this subsection or created, established, or controlled by an entity specified in paragraph (a) or (b) of this subsection;

(d) Every public school district in the Commonwealth of Kentucky; and

(e) Every public institution of postsecondary education, including every public university in the Commonwealth of Kentucky and public college of the entire Kentucky Community and Technical College System;

(2) "Commonwealth Office of Technology" means the office established by KRS 42.724;

(3) "Encryption" means the conversion of data using technology that:

(a) Meets or exceeds the level adopted by the National Institute of Standards Technology as part of the Federal Information Processing Standards: and

(b) Renders the data indecipherable without the associated cryptographic key to decipher the data;

(4) "Law enforcement agency" means any lawfully organized investigative agency, sheriff's office, police unit, or police force of federal, state, county, urban-county government, charter county, city, consolidated local government, unified local government, or any combination of these entities, responsible for the detection of crime and the enforcement of the general criminal federal and state laws;

(5) "Nonaffiliated third party" means any person that:

(a) Has a contract or agreement with an agency; and

(b) Receives personal information from the agency pursuant to the contract or agreement;

(6) "Personal information" means an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with one (1) or more of the following data elements:

(a) An account number, credit card number,~~[or]~~ debit card number***, user name, or e-mail address*** that, in combination with any required security code, ***security question and answer,*** access code, or password, would permit access to an account;

(b) A Social Security number;

(c) A taxpayer identification number that incorporates a Social Security number;

(d) A driver's license number, state identification card number, or other individual identification number issued by any agency;

(e) A passport number or other identification number issued by the United States government; or

(f) Individually identifiable health information as defined in 45 C.F.R. sec. 160.103, except for education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g;

(7) (a) "Public record or record," as established by KRS 171.410, means all books, papers, maps, photographs, cards, tapes, disks, diskettes, recordings, and other

documentary materials, regardless of physical form or characteristics, which are prepared, owned, used, in the possession of, or retained by a public agency.

(b) "Public record" does not include any records owned by a private person or corporation that are not related to functions, activities, programs, or operations funded by state or local authority;

(8) "Reasonable security and breach investigation procedures and practices" means data security procedures and practices developed in good faith and set forth in a written security information policy; and

(9) (a) "Security breach" means:

1. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises**,** or the agency or nonaffiliated third party reasonably believes may compromise**,** the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals; or

2. The unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of encrypted records or data containing personal information along with the confidential process or key to unencrypt the records or data that compromises**,** or the agency or nonaffiliated third party reasonably believes may compromise**,** the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one (1) or more individuals.

(b) "Security breach" does not include the good-faith acquisition of personal information by an employee, agent, or nonaffiliated third party of the agency for the purposes of the agency if the personal information is**:**

1. Used for a purpose related to the agency**;** and

2. ~~[Is]~~Not subject to unauthorized disclosure.

➔Section 2. KRS 61.933 is amended to read as follows:

(1) (a) Any agency that collects, maintains, or stores personal information that determines or is notified of a security breach relating to personal information collected, maintained, or stored by the agency or by a nonaffiliated third party on behalf of the agency shall as soon as possible, but within seventy-two (72) hours of determination or notification of the security breach:

1. Notify the commissioner of the Kentucky State Police, the Auditor of Public Accounts, and the Attorney General. In addition, an agency shall notify the secretary of the Finance and Administration Cabinet or his or her designee if an agency is an organizational unit of the executive branch of state government; notify the commissioner of the Department for Local Government if the agency is a unit of government listed in KRS 61.931(1)(b) or (c) that is not an organizational unit of the executive branch of state government; notify the commissioner of the Kentucky Department of Education if the agency is a public school district listed in KRS 61.931(1)(d); and notify the president of the Council on Postsecondary Education if the agency is an educational entity listed under KRS 61.931(1)(e). Notification shall be in writing on a form developed by the Commonwealth Office of Technology. The Commonwealth Office of Technology shall promulgate administrative regulations under KRS 61.931 to 61.934 regarding the contents of the form; and

2. Begin conducting a reasonable and prompt investigation in accordance with the security and breach investigation procedures and practices referenced in KRS 61.932(1)(b) to determine whether the security breach has resulted in or is likely to result in the misuse of the personal

information.

(b) Upon conclusion of the agency's investigation:

1. If the agency determined that a security breach has occurred and that the misuse of personal information has occurred or is reasonably likely to occur, the agency shall:

a. Within forty-eight (48) hours of completion of the investigation, notify in writing all officers listed in paragraph (a)1. of this subsection, and the commissioner of the Department for Libraries and Archives, unless the provisions of subsection (3) of this section apply;

b. Within thirty-five (35) days of providing the notifications required by subdivision a. of this subparagraph, notify all individuals impacted by the security breach as provided in subsection (2) of this section, unless the provisions of subsection (3) of this section apply; and

c. If the number of individuals to be notified exceeds one thousand (1,000), the agency shall notify, at least seven (7) days prior to providing notice to individuals under subdivision b. of this subparagraph, the Commonwealth Office of Technology if the agency is an organizational unit of the executive branch of state government, the Department for Local Government if the agency is a unit of government listed under KRS 61.931(1)(b) or (c) that is not an organizational unit of the executive branch of state government, the Kentucky Department of Education if the agency is a public school district listed under KRS 61.931(1)(d), or the Council on Postsecondary Education if the agency is an educational entity listed under KRS 61.931(1)(e); and notify all

consumer credit reporting agencies included on the list maintained by the Office of the Attorney General that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. sec. 1681a(p), of the timing, distribution, and content of the notice; or

2. If the agency determines that the misuse of personal information has not occurred and is not likely to occur, the agency is not required to give notice, but shall maintain records that reflect the basis for its decision for a retention period set by the State Archives and Records Commission as established by KRS 171.420. The agency shall notify the appropriate entities listed in paragraph (a)1. of this subsection that the misuse of personal information has not occurred.

(2) (a) The provisions of this subsection establish the requirements for providing notice to individuals under subsection (1)(b)1.b. of this section. Notice shall be provided as follows:

1. Conspicuous posting of the notice on the Web site of the agency;
2. Notification to regional or local media if the security breach is localized, and also to major statewide media if the security breach is widespread, including broadcast media, such as radio and television; and
3. Personal communication to individuals whose data has been breached using the method listed in subdivision a., b., or c. of this subparagraph that the agency believes is most likely to result in actual notification to those individuals, if the agency has the information available:
   a. In writing, sent to the most recent address for the individual as reflected in the records of the agency;
   b. By electronic mail, sent to the most recent electronic mail address for the individual as reflected in the records of the agency, unless

the individual has communicated to the agency in writing that they do not want email notification; or

c. By telephone, to the most recent telephone number for the individual as reflected in the records of the agency.

(b) The notice shall be clear and conspicuous, and shall include:

1. To the extent possible, a description of the categories of information that were subject to the security breach, including the elements of personal information that were or were believed to be acquired;

2. Contact information for the notifying agency, including the address, telephone number, and toll-free number if a toll-free number is maintained;

3. A description of the general acts of the agency, excluding disclosure of defenses used for the protection of information, to protect the personal information from further security breach; and

4. The toll-free numbers, addresses, and Web site addresses, along with a statement that the individual can obtain information from the following sources about steps the individual may take to avoid identity theft, for:

a. The major consumer credit reporting agencies;

b. The Federal Trade Commission; and

c. The Office of the Kentucky Attorney General.

(c) The agency providing notice pursuant to this subsection shall cooperate with any investigation conducted by the agencies notified under subsection (1)(a) of this section and with reasonable requests from the Office of Consumer Protection of the Office of the Attorney General, consumer credit reporting agencies, and recipients of the notice, to verify the authenticity of the notice.

(3) (a) The notices required by subsection (1) of this section shall not be made if, after consultation with a law enforcement agency, the agency receives a

written request from a law enforcement agency for a delay in notification because the notice may impede a criminal investigation. The written request may apply to some or all of the required notifications, as specified in the written request from the law enforcement agency. Upon written notification from the law enforcement agency that the criminal investigation has been completed, or that the sending of the required notifications will no longer impede a criminal investigation, the agency shall send the notices required by subsection (1)(b)1. of this section.

(b) The notice required by subsection (1)(b)1.b. of this section may be delayed if the agency determines that measures necessary to restore the reasonable integrity of the data system cannot be implemented within the timeframe established by subsection (1)(b)1.b. of this section, and the delay is approved in writing by the Office of the Attorney General. If notice is delayed pursuant to this subsection, notice shall be made immediately after actions necessary to restore the integrity of the data system have been completed.

(4) Any waiver of the provisions of this section is contrary to public policy and shall be void and unenforceable.

(5) This section shall not apply to:

(a) Personal information that has been redacted;

(b) Personal information disclosed to a federal, state, or local government entity, including a law enforcement agency or court, or their agents, assigns, employees, or subcontractors, to investigate or conduct criminal investigations and arrests or delinquent tax assessments, or to perform any other statutory duties and responsibilities;

(c) Personal information that is publicly and lawfully made available to the general public from federal, state, or local government records;

(d) Personal information that an individual has consented to have publicly

disseminated or listed; or

(e) Any document recorded in the records of either a county clerk or circuit clerk of a county, or in the records of a United States District Court.

(6) ***(a)*** The Office of the Attorney General may bring an action in the Franklin Circuit Court against an agency or a nonaffiliated third party that is not an agency, or both, for injunctive relief, and for other legal remedies against a nonaffiliated third party that is not an agency to enforce the provisions of KRS 61.931 to 61.934.~~[Nothing in KRS 61.931 to 61.934 shall create a private right of action]~~

(b) 1. Within one (1) year after any action of the Attorney General has been terminated or within two (2) years after the violation of this chapter, whichever is later, any person injured by a violation of KRS 61.931 to 61.934 shall have a civil cause of action in the Franklin Circuit Court to enjoin further violations, and to recover the actual damages sustained, together with the costs of the lawsuit, including reasonable attorney's fees.

2. The court may, in its discretion, award actual damages, award reasonable attorney's fees and costs, and provide such equitable relief as it deems necessary or proper.

3. Upon commencement of any action brought under subparagraph 1. of this paragraph, the clerk of the court shall mail a copy of the complaint or other initial pleading to the Attorney General and, upon entry of any judgment or decree in the action, shall mail a copy of the judgment or decree to the Attorney General.

➔Section 3. KRS 365.732 is amended to read as follows:

(1) As used in this section, unless the context otherwise requires:

(a) "Breach of the security of the system" means***:***

1. Unauthorized acquisition of ***or access to*** unencrypted and unredacted ***records or***~~[computerized]~~ data that compromises***, or that the information holder reasonably believes may compromise,*** the security, confidentiality, or integrity of personally identifiable information maintained by the information holder***; or***

2. Unauthorized acquisition of or access to encrypted records or data along with the associated cryptographic key to decipher the data that compromises, or that the information holder reasonably believes may compromise, the security, confidentiality, or integrity of personally identifiable information maintained by the information holder~~[as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky]~~.

Good-faith acquisition of personally identifiable information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system if the personally identifiable information is not used or subject to further unauthorized disclosure;

(b) ***"Encryption" means the conversion of data using technology that:***

1. Meets or exceeds the level adopted by the National Institute of Standards and Technology as part of the Federal Information Processing Standards; and

2. Renders the data indecipherable without the associated cryptographic key to decipher the data;

(c) "Information holder" means any person or business entity that conducts business in this state;~~[and]~~

(d)~~[(c)]~~ "Personally identifiable information" means an individual's first name or

first initial and last name***, or unique biometric or genetic print or image,*** in combination with any one (1) or more of the following data elements, when the~~[name or]~~ data element is not redacted:

1. Social Security number;

2. Driver's license number***, state identification card number, passport number, or other individual identification number issued by a state or federal government agency***;~~[or]~~

3. Account number~~,[or]~~ credit or debit card number, ***user name, or e-mail address,*** in combination with any required security code, ***security question and answer,*** access code, or password to permit access to an individual's~~[financial]~~ account***; or***

4. Taxpayer identification number that incorporates a Social Security number;

(e) "Record" means information that is inscribed on a tangible medium or which is stored in an electronic or other medium and is retrievable in perceivable form; and

(f) "Third-party agent" means any person who:

1. Has a contract or agreement with an information holder; and

2. Receives personally identifiable information from the information holder pursuant to the contract or agreement.

(2) ***(a)*** Any information holder shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the ***personally identifiable information collected, maintained, or stored by the information holder***~~[data]~~, to any resident of Kentucky whose~~[unencrypted]~~ personal information was, or is reasonably believed to have been, ***accessed or*** acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, ***no more than thirty-***

five (35) days after the breach was discovered, consistent with the legitimate needs of law enforcement[,] as provided in subsection (4) of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Such notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state, and local agencies responsible for law enforcement, the information holder reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired or accessed.

(3) Any ***third-party agent***[information holder] that ***receives records or***[maintains computerized] data that ***include***[includes] personally identifiable information[that the information holder does not own] shall notify the[owner or licensee of the] information ***holder*** of any breach of the security of the data as soon as reasonably practicable following discovery***, but within seventy-two (72) hours***, if the personally identifiable information was, or is reasonably believed to have been, ***accessed or*** acquired by an unauthorized person.

(4) The notification required by this section may be delayed if ***the information holder receives a written request for a delay from*** a law enforcement agency ***because***[determines that] the notification will impede a criminal investigation. The notification required by this section shall be made[promptly] after the law enforcement agency determines that it will not compromise the investigation.

(5) For purposes of this section, notice may be provided by one (1) of the following methods:

(a) Written notice;

(b) ***Telephone notice;***

(c) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. sec. 7001,

unless the breach of the security involved an electronic mail address with additional information which would permit access to the electronic mail account, in which case notice shall not be sent to that electronic mail address; or

(d)~~[(c)]~~ Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the information holder does not have sufficient contact information. Substitute notice shall consist of all of the following:

1. E-mail notice, when the information holder has an e-mail address for the subject persons;
2. Conspicuous posting of the notice on the information holder's Internet Web site page, if the information holder maintains a Web site page; and
3. Notification to major statewide media.

(6) Notwithstanding subsection (5) of this section, an information holder that maintains its own notification procedures as part of an information security policy for the treatment of personally identifiable 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 of the system.

(7) If a person discovers circumstances requiring notification pursuant to this section of more than one thousand (1,000) persons at one (1) time, the person shall also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. sec. 1681a, of the timing, distribution, and content of the notices.

(8) The provisions of this section and the requirements for nonaffiliated third parties in

KRS Chapter 61 shall not apply to any person who is subject to the provisions of Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended, or the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended, or any agency of the Commonwealth of Kentucky or any of its local governments or political subdivisions.

(9) (a) Any person injured by a violation of this section may institute a civil action to recover damages.

(b) Any information holder or third-party agent that violates, proposes to violate, or has violated any provision of this section may be enjoined in a civil action.

(c) The rights and remedies available under this section shall be cumulative to each other and to any other rights and remedies available under law.