AN ACT relating to the security of personal information and declaring an emergency.

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

➔Section 1. KRS 367.363 is amended to read as follows:

As used in KRS 367.363 to 367.365, unless the context requires otherwise:

(1) "Clear and proper identification" means information generally deemed sufficient to identify a person. If the consumer is unable to reasonably identify himself or herself with such information, a consumer reporting agency may require additional information to verify his or her identity;

(2) "Consumer" means any natural person who is a resident of Kentucky;

(3) ~~[(2)]~~ "Consumer report" means a consumer report, as defined in the ~~[federal]~~Fair Credit Reporting Act, 15 U.S.C. sec. 1681a(d);

(4) ~~[(3)]~~ "Consumer reporting agency" means a consumer reporting agency as defined by the ~~[federal]~~Fair Credit Reporting Act, 15 U.S.C. sec. 1681a(f). "Consumer reporting agency" shall not mean a check acceptance service which provides check approval and guarantees services to merchants;~~[and]~~

(5) "Credit monitoring" means a service that, at a minimum, provides for the daily monitoring of a consumer's consumer reports for the purpose of alerting the consumer to signs of possible fraud, including the following:

(a) Providing the consumer, at no charge, at least three (3) consumer reports each year from each nationwide consumer reporting agency;

(b) Monitoring the consumer's consumer report at each nationwide consumer reporting agency; and

(c) Alerting the consumer by telephone, e-mail, or text when there are changes in the consumer's consumer report;

(6) "Encrypt" has the same meaning as in Section 6 of this Act;

(7) "Nationwide consumer reporting agency" means a consumer reporting agency

that compiles and maintains files on consumers on a nationwide basis as defined by the Fair Credit Reporting Act, 15 U.S.C. sec. 1681a(p);

(8) "Personally identifiable information" means a consumer's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with any one (1) or more of the following data elements:

(a) An account number, credit card number, debit card number, user name, or e-mail address with or without any security code, security question and answer, access code, or password that permits access to a consumer's account;

(b) A Social Security number;

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

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

(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;

(9) (a) "Security breach" means the unauthorized acquisition, distribution, disclosure, destruction, or manipulation of, or access to, a consumer reporting agency's records or data that:

1. Compromises, or the agency reasonably believes may compromise, the security, confidentiality, or integrity of personally identifiable information; and

2. Results in the likelihood of harm to one (1) or more consumers.

(b) "Security breach" does not include:

1. The good-faith acquisition of or access to personally identifiable information by an employee or agent of the consumer reporting

agency if the information is used for a lawful purpose and is not subject to unauthorized disclosure; or

2. The acquisition, distribution, or disclosure of, or access to, encrypted or redacted records or data without the accompanying acquisition of or reasonable ability to access or discover the confidential process or key necessary to unencrypt or decipher the records or data;

(10) ~~[(4)]~~ "Security freeze" means a notice placed on a consumer file, at the request of the consumer and subject to certain exceptions, that prohibits a consumer reporting agency from releasing the consumer's consumer report or credit score relating to the extension of credit without the express authorization of the consumer***; and***

(11) "Third-party agent" means any person that possesses or controls personally identifiable information on behalf of a consumer reporting agency pursuant to a contract or agreement with the consumer reporting agency.

➔Section 2. KRS 367.3645 is amended to read as follows:

(1) For the purposes of this section:

(a) "Protected person" means an individual who is under sixteen (16) years of age at the time a request for the placement of a security freeze is made, or who is an incapacitated person or other person for whom a guardian or conservator has been appointed;

(b) "Record" means a compilation of information which:

1. Identifies a protected person;

2. Is created by a consumer reporting agency solely for the purpose of complying with this section; and

3. Is not created or used to consider the protected person's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living;

(c) "Representative" means a person who provides to a consumer reporting

agency sufficient proof of authority to act on behalf of a protected person; and

(d) "Sufficient proof of authority" means documentation that shows a representative has authority to act on behalf of a protected person, including but not limited to:

1. A court order granting custodianship, guardianship, or conservatorship;
2. A birth certificate;
3. A lawfully executed and valid power of attorney; or
4. A written, notarized statement signed by a representative that expressly describes the authority of the representative to act on behalf of a protected person.

(2) A consumer reporting agency shall place a security freeze on a protected person's record or ***consumer***~~[credit]~~ report if:

(a) The consumer reporting agency receives a request from the protected person's representative for the placement of the security freeze; and

(b) The protected person's representative:

1. Submits the request to the consumer reporting agency ***using the method that the agency has established to receive security freeze requests***~~[at the address designated by the consumer reporting agency to receive the request]~~;
2. Provides to the consumer reporting agency clear and proper identification of the protected person and the representative;
3. Provides to the consumer reporting agency sufficient proof of authority to act on behalf of the protected person; and
4. Pays to the consumer reporting agency a fee as prescribed in subsection (8) of this section.

(3) If a consumer reporting agency does not have a file pertaining to a protected person when the consumer reporting agency receives a request pursuant to subsection (2) of

this section, the consumer reporting agency shall create a record for the protected person.

(4) Within thirty (30) days after receiving a request pursuant to this section, a consumer reporting agency shall place a security freeze on the protected person's record or ***consumer***~~[credit]~~ report.

(5) Unless a security freeze is removed pursuant to subsection (7) or (10) of this section, a consumer reporting agency may not release the protected person's ***consumer***~~[credit]~~ report, any information derived from the protected person's ***consumer***~~[credit]~~ report, or any record created for the protected person.

(6) A security freeze that is placed on a protected person's record or ***consumer***~~[credit]~~ report placed under this section remains in effect until either:

(a) The protected person or the protected person's representative requests that the consumer reporting agency remove the security freeze pursuant to subsection (7) of this section; or

(b) The security freeze is removed pursuant to subsection (10) of this section.

(7) (a) To remove a security freeze for a protected person, the protected person or the protected person's representative shall submit a request for the removal of the security freeze to the consumer reporting agency at the address designated by the consumer reporting agency to receive the request, and pay a fee as prescribed in subsection (8) of this section. In addition:

1. If the protected person requested the removal of the security freeze, the protected person shall provide to the consumer reporting agency ***both***~~[either]~~ of the following:

a. Proof that the protected person's representative no longer has sufficient proof of authority to act on behalf of the protected person; ***and***~~[or]~~

b. Clear and proper identification of the protected person; and

2. If the protected person's representative requested the removal of the security freeze on behalf of the protected person, the protected person's representative shall provide to the consumer reporting agency both of the following:

a. Clear and proper identification of the protected person and the representative; and

b. Sufficient proof of authority to act on behalf of the protected person.

(b) Within thirty (30) days after receiving a request to remove a security freeze placed pursuant to subsection (2) of this section, the consumer reporting agency shall remove the security freeze for the protected person.

(8) A consumer reporting agency may charge a fee for each placement or removal of a security freeze on a protected person's record or ***consumer***~~[credit]~~ report. The fee ***shall***~~[may]~~ not exceed ten dollars ($10).

(9) Notwithstanding subsection (8) of this section, a consumer reporting agency ***shall***~~[may]~~ not charge ***a***~~[any]~~ fee under this section if:

(a) The protected ***person or the protected person's representative has received a notification of a security breach pursuant to Section 3, 5, or 8 of this Act that affects the protected person and, upon request, provides a copy of the notification to the consumer reporting agency;***

(b) The protected person is a victim of identity theft and, upon request, the protected person or the protected person's representative provides a copy of a ***valid*** police report to the consumer reporting agency~~[alleging that the protected person has been a victim of an offense involving identity theft]~~;~~[or]~~

(c)~~[(b)]~~ A request for the placement or removal of a security freeze is for a protected person who is under sixteen (16) years of age at the time of the request and the consumer reporting agency has a ***consumer***~~[credit]~~ report

pertaining to the protected person***; or***

(d) The protected person or the protected person's representative has received a notification from another consumer reporting agency that a security freeze has been or may be placed on the protected person's record or consumer report at no charge and upon request, provides a copy of the notification to the consumer reporting agency.

(10) A consumer reporting agency may remove a security freeze for a protected person or may delete a protected person's record if the security freeze was placed or the record was created based on a material misrepresentation of fact by the protected person or the protected person's representative.

(11) Any person who willfully fails to comply with any requirement imposed under this section with respect to any ***protected person***~~[consumer]~~ is liable to that ***person***~~[consumer]~~ in an amount equal to the sum of:

(a) Any actual damages sustained by the consumer as a result of the failure;

(b) Any liquidated damages of not less than one hundred dollars ($100) and not more than one thousand dollars ($1,000);

(c) Any punitive damages as the court may allow; and

(d) In the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

(12) Any person, other than the named individual or individuals in the report, who obtains a consumer report, requests a security freeze, requests the temporary lift of a freeze, or requests the removal of a security freeze from a consumer reporting agency under false pretenses or in an attempt to violate federal or state law shall be liable to the consumer reporting agency for actual damages sustained by the consumer reporting agency or one thousand dollars ($1,000), whichever is greater.

(13) This section does not apply to a protected person's ***consumer***~~[credit]~~ report or

record provided to:

(a) A federal, state, or local governmental entity, including a law enforcement agency, or court, or their agents or assigns;

(b) A private collection agency for the sole purpose of assisting in the collection of an existing debt of the consumer who is the subject of the consumer report requested;

(c) A person or entity, or a subsidiary, affiliate, or agent of that person or entity, or an assignee of a financial obligation owing by the consumer to that person or entity, or a prospective assignee of a financial obligation owing by the consumer to that person or entity in conjunction with the proposed purchase of the financial obligation, with which the consumer has or had prior to assignment an account or contract, including a demand deposit account, or to whom the consumer issued a negotiable instrument, for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or negotiable instrument. For purposes of this paragraph, "reviewing the account" includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements;

(d) A person~~[,]~~ for the purposes of prescreening as provided by the~~[federal]~~ Fair Credit Reporting Act, 15 U.S.C. secs. 1681 et seq.;

(e) A consumer reporting agency for the purposes of providing a consumer with a copy of his or her own report on ***the consumer's***~~[his or her]~~ request;

(f) A child support enforcement agency;

(g) A consumer reporting agency that acts only as a reseller of credit information by assembling and merging information contained in the database of another consumer reporting agency or multiple credit reporting agencies and does not maintain a permanent database of credit information from which new consumer reports are produced. However, a consumer reporting agency acting

as a reseller shall honor any security freeze placed on a consumer report by another consumer reporting agency;

(h) A check services or fraud prevention services company ***that*** ~~[, which]~~ issues reports on incidents of fraud or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payments;

(i) A deposit account information service company ***that*** ~~[, which]~~ issues reports regarding account closures due to fraud, substantial overdrafts, ATM abuse, or similar negative information regarding a consumer to inquiring banks or other financial institutions for use only in reviewing a consumer request for a deposit account at the inquiring bank or financial institution;

(j) Any person or entity using a consumer report in preparation for a civil or criminal action, or an insurance company in investigation of a claim; or

(k) 1. Any insurance company for setting or adjusting a rate or underwriting for property and casualty insurance purposes; or

2. Any consumer reporting agency database or file which consists solely of consumer information concerning, and used solely for:

a. Criminal record information;

b. Personal loss history information;

c. Fraud prevention or detection;

d. Employment screening; or

e. Tenant screening.

➔Section 3. KRS 367.365 is amended to read as follows:

(1) A consumer reporting agency shall encrypt electronic data contained in:

(a) The consumer file of a consumer; and

(b) Each consumer report of a consumer both:

1. In the possession or control of the consumer reporting agency or a

third-party agent; and

2. During transfer between the consumer reporting agency or third-party agent and the consumer or any third party.

(2)~~[(1)]~~ (a) A consumer may elect to place a security freeze on the consumer's consumer report by written request~~[, sent by certified mail, that includes clear and proper identification,]~~ to a consumer reporting agency at an address designated by the consumer reporting agency to receive ***security freeze requests, or by the use of telephone, fax, or Web-based or other electronic method that the consumer reporting agency has established to receive security freeze requests. A request made pursuant to this subsection shall include clear and proper identification***~~[such request]~~. A consumer reporting agency shall place a security freeze on a consumer's consumer report no later than ten (10) business days after receiving a~~[written]~~ request ***made pursuant to this subsection*** for the ***placement of a*** security freeze from the consumer.

(b) When a security freeze is in place, information from a consumer's consumer report shall not be released to a third party without prior express authorization from the consumer. This subsection does not prevent a consumer reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's consumer report.

(3)~~[(2)]~~ The consumer reporting agency shall, no later than ten (10) business days after the date the agency receives the request for a security freeze, provide the consumer with a unique personal identification number or password to be used by the consumer when providing authorization for the access to his or her credit file for a specific period of time. In addition, the consumer reporting agency shall simultaneously provide to the consumer in writing the process of placing, removing, and temporarily lifting a security freeze and the process for allowing access to information from the consumer's credit file for a specific period while the security

freeze is in effect.

(4)~~[(3)]~~ A consumer may request~~[in writing]~~ a replacement personal identification number or password ***in the same manner utilized in subsection (2) of this section to request the initial security freeze and shall also include clear and proper identification***.~~[The request shall comply with the requirements for requesting a security freeze under subsection (1) of this section.]~~ ***No later than ten (10) business days after the date the consumer reporting agency receives the request for a replacement personal identification number or password,*** the consumer reporting agency shall~~[, not later than the tenth business day after the date the agency receives the request for a replacement personal identification number or password,]~~ provide the consumer with a new, unique personal identification number or password to be used by the consumer instead of the number or password that was provided under subsection ***(3)***~~[(2)]~~ of this section.

(5)~~[(4)]~~ If a third party requests access to a consumer report on which a security freeze is in effect, and this request is in connection with an application for credit, the third party may treat the application as incomplete.

(6)~~[(5)]~~ If the consumer wishes to allow his ***or her*** consumer report or credit score to be accessed for a specific period of time while a freeze is in place, the consumer shall contact the consumer reporting agency and request that the freeze be temporarily lifted and provide the following:

(a) Clear and proper identification;

(b) The unique personal identification number or password provided by the consumer reporting agency pursuant to subsection ~~[(2) or]~~(3) ***or (4)*** of this section; and

(c) The proper information regarding the time period for which the report shall be available to users of the consumer report.

(7)~~[(6)]~~ A consumer reporting agency that receives a request from a consumer to

temporarily lift a freeze on a consumer report pursuant to subsection ***(6)***~~[(5)]~~ of this section shall comply with the request no later than three (3) business days after receiving the request. A consumer reporting agency may develop procedures involving the use of telephone, fax, the Internet, or other electronic ***method***~~[media]~~ to receive and process a request from a consumer to temporarily lift a freeze on a consumer report or credit score pursuant to subsection ***(6)***~~[(5)]~~ of this section in an expedited manner.

(8)~~[(7)]~~ A consumer reporting agency shall remove or temporarily lift a freeze placed on a consumer's consumer report only~~[in the following cases]~~:

(a) Upon ***the consumer's***~~[consumer]~~ request ***made pursuant to subsection (6) or (9) of***~~[as provided in]~~ this section; or

(b) If the~~[consumer's]~~ consumer report was frozen due to a material misrepresentation of fact by the consumer. If a consumer reporting agency intends to remove a freeze upon a~~[consumer's]~~ consumer report pursuant to this paragraph, the consumer reporting agency shall notify the consumer in writing prior to removing the freeze on the~~[consumer's]~~ consumer report.

(9)~~[(8)]~~ A security freeze shall remain in place until the consumer requests that the security freeze be removed, ***or the consumer reporting agency has notified the consumer in writing that it is removing the freeze due to a misrepresentation of fact by the consumer pursuant to subsection (8)(b) of this section***~~[but no longer than seven (7) years from the date the security freeze was put in place]~~. A consumer reporting agency shall remove a security freeze within three (3) business days of receiving***:***

(a) ~~[ ]~~A request for removal from the consumer***; and***~~[, who provides]~~

(b) Both of the following:

1.~~[(a)]~~ Clear and proper identification; and

2.~~[(b)]~~ The unique personal identification number or password provided

by the consumer reporting agency.

(10) ~~[(9)]~~ A security freeze does not apply to a consumer report provided to:

(a) A federal, state, or local governmental entity, including a law enforcement agency, or court, or their agents or assigns;

(b) A private collection agency for the sole purpose of assisting in the collection of an existing debt of the consumer who is the subject of the consumer report requested;

(c) A person or entity, or a subsidiary, affiliate, or agent of that person or entity, or an assignee of a financial obligation owing by the consumer to that person or entity, or a prospective assignee of a financial obligation owing by the consumer to that person or entity in conjunction with the proposed purchase of the financial obligation, with which the consumer has or had prior to assignment an account or contract, including a demand deposit account, or to whom the consumer issued a negotiable instrument, for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or negotiable instrument. For purposes of this paragraph, "reviewing the account" includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements;

(d) A subsidiary, affiliate, agent, assignee, or prospective assignee of a person to whom access has been granted under subsection ***(6)*** ~~[(5)]~~ of this section for the purposes of facilitating the extension of credit;

(e) A person~~[,]~~ for the purposes of prescreening as provided by the~~[federal]~~ Fair Credit Reporting Act***, 15 U.S.C. secs. 1681 et seq.***;

(f) A consumer reporting agency for the purposes of providing a consumer with a copy of his ***or her*** own report on ***the consumer's*** ~~[his]~~ request;

(g) A child support enforcement agency;

(h) A consumer reporting agency that acts only as a reseller of credit information

by assembling and merging information contained in the database of another consumer reporting agency or multiple credit reporting agencies and does not maintain a permanent database of credit information from which new consumer reports are produced. However, a consumer reporting agency acting as a reseller shall honor any security freeze placed on a consumer report by another consumer reporting agency;

(i) A check services or fraud prevention services company ***that***~~[, which]~~ issues reports on incidents of fraud or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payments;

(j) A deposit account information service company ***that***~~[, which]~~ issues reports regarding account closures due to fraud, substantial overdrafts, ATM abuse, or similar negative information regarding a consumer to inquiring banks or other financial institutions for use only in reviewing a consumer request for a deposit account at the inquiring bank or financial institution;

(k) Any person or entity using a consumer report in preparation for a civil or criminal action, or an insurance company in investigation of a claim; or

(l) Any insurance company for setting or adjusting a rate or underwriting for property and casualty insurance purposes.

(11)~~[(10)]~~ A consumer reporting agency may impose a reasonable charge on a consumer for initially placing, temporarily lifting, or removing a security freeze on a consumer file. The amount of the charge may not exceed ten dollars ($10). On January 1 of each year, a consumer reporting agency may increase the charge for placing a security ***freeze***~~[alert]~~. The increase shall be based proportionally on changes to the Consumer Price Index for All Urban Consumers as determined by the United States Department of Labor with fractional changes rounded to the nearest twenty-five cents ($0.25).~~[An exception shall be allowed whereby the consumer will be~~

~~charged zero dollars by the consumer reporting agency placing the security freeze if~~]

(12) Notwithstanding subsection (11) of this section, a consumer reporting agency shall not charge a fee under this section if:

(a) The consumer***:***

1. Has received a notification:

a. Of a security breach pursuant to subsection (14) of this section, or Section 5 or 8 of this Act that affects the consumer; or

b. From another consumer reporting agency that a security freeze has been or may be placed on the consumer's consumer report at no charge; or

2. Is a victim of identity theft***;*** and[~~, ~~]

(b) Upon[~~ the~~] request[~~ of the consumer reporting agency~~], ***the consumer*** provides the consumer reporting agency with a ***copy of a*** valid police report ***or the notification received pursuant to paragraph (a)1. of this subsection***.

(13) (a)[~~(11)~~] If a security freeze is in place, a consumer reporting agency shall not change any of the following official information in a consumer report without sending a written confirmation of the change to the consumer within thirty (30) days of the change being posted to the consumer's file:

1.[~~(a)~~] Name;

2.[~~(b)~~] Date of birth;

3.[~~(c)~~] Social Security number; and

4.[~~(d)~~] Address.

(b) Written confirmation is not required for technical modifications of a consumer's official information, including name and street abbreviations, complete spellings, or transposition of numbers or letters. In the case of an address change, the written confirmation shall be sent to both the new address

and to the former address.

(14) For each consumer affected by a security breach, the consumer reporting agency whose data has been breached shall:

(a) Notify the consumer of the security breach as soon as possible and without unreasonable delay in compliance with the requirements of subsections (4) to (7) of Section 5 of this Act; and

(b) For a period of five (5) years following the breach:

1. Provide or offer credit monitoring, either directly or from a third party, to the consumer at no cost to the consumer; or

2. Reimburse the consumer for credit monitoring purchased by the consumer.

(15) An individual who has been notified of a security breach pursuant to subsection (14) of this section, or Section 5 or 8 of this Act, including but not limited to a protected person or his or her representative as defined in Section 2 of this Act, who places a security freeze with a nationwide consumer reporting agency shall have the option to have notice of the placement of the security freeze sent to any other nationwide consumer reporting agency and applied to the corresponding consumer report for that agency.

(16) A third-party agent shall notify the consumer reporting agency of any security breach relating to the consumer reporting agency's records or data as soon as reasonably practicable, but not later than seventy-two (72) hours, following discovery.

(17) A consumer reporting agency shall comply with subsections (3) and (9) of Section 5 of this Act.

(18) ~~[(12)]~~ Any person who willfully fails to comply with any requirement imposed under this section with respect to any consumer is liable to that consumer in an amount equal to the sum of:

(a) Any actual damages sustained by the consumer as a result of the failure;

(b) Any liquidated damages of not less than one hundred dollars ($100) and not more than one thousand dollars ($1,000);

(c) Any punitive damages as the court may allow; and

(d) In the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

(19) ~~[(13)]~~ Any person, other than the named individual or individuals in the report, who obtains a consumer report, requests a security freeze, requests the temporary lift of a freeze, or the removal of a security freeze from a consumer reporting agency under false pretenses or in an attempt to violate federal or state law shall be liable to the consumer reporting agency for actual damages sustained by the consumer reporting agency or one thousand dollars ($1,000), whichever is greater.

(20) ~~[(14)]~~ Any person who is negligent in failing to comply with any requirement imposed under this section with respect to any consumer is liable to that consumer in an amount equal to the sum of:

(a) Any actual damages sustained by the consumer as a result of the failure; and

(b) In the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

(21) An individual shall not, as a condition of exercising his or her rights under any of the provisions of this section, be required to:

(a) Waive any right to a private right of action; or

(b) Agree to submit to a binding arbitration procedure.

(22) ~~[(15)]~~ Nothing in KRS 367.363 to 367.365 shall be construed to limit or restrict the exercise of powers or the performance of the duties of the Attorney General authorized under any other provision of law to bring or seek redress for persons that

violate KRS 367.363 to 367.365.

➔Section 4. KRS 365.720 is amended to read as follows:

As used in KRS 365.720 to ***365.732***~~[365.730]~~, unless the context requires otherwise:

(1) "Business" means a sole proprietorship, partnership, corporation, limited liability company, association, or other entity, however organized and whether or not organized to operate at a profit. "Business" shall not mean a bank as defined in 12 U.S.C. sec. 1813(a) or Subtitles 1, 2, and 3 of KRS Chapter 286, a credit union as defined in 12 U.S.C. sec. 1752 or Subtitle 6 of KRS Chapter 286, a savings association as defined in 12 U.S.C. sec. 1813(b), or an association as defined in Subtitle 5 of KRS Chapter 286. The term includes an entity that destroys records;

(2) "Customer" means an individual who provides ***personally identifiable***~~[personal]~~ information to a business for the purpose of purchasing or leasing a product or obtaining a service for business;

(3) "Individual" means a natural person;

(4) "Personally identifiable 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 any one (1) or more of the following data elements:***

(a) An account number, credit card number, debit card number, user name, or e-mail address with or without any security code, security question and answer, access code, or password that permits access to an individual's account;

(b) A Social Security number;

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

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

(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~~[means data capable of being associated with a particular customer through one (1) or more identifiers, including but not limited to a customer's name, address, telephone number, electronic mail address, fingerprints, photographs or computerized image, Social Security number, passport number, driver identification number, personal identification card number or code, date of birth, medical information, financial information, tax information, and disability information]~~; and

(5) "Records" means any material, regardless of the physical form, on which information is recorded or preserved by any means, including in written or spoken words, graphically depicted, printed, or electromagnetically transmitted.

➔Section 5. KRS 365.732 is amended to read as follows:

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

(a) ***"Encrypt" has the same meaning as in Section 6 of this Act***~~["Breach of the security of the system" means unauthorized acquisition of unencrypted and unredacted computerized data that compromises 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) "Information holder" means any person or business entity that conducts business in this state; and

(c) ***1. "Security Breach" means the unauthorized acquisition, distribution, or disclosure, destruction, or manipulation of, or access to, an information holder's records or data that:***

a. Compromises, or the information holder reasonably believes may compromise, the security, confidentiality, or integrity of personally identifiable information; and

b. Results in the likelihood of harm to one (1) or more individuals.

2. "Security breach" does not include:

a. The good-faith acquisition of or access to personally identifiable information by an employee or agent of the information holder if the information is used for a lawful purpose and is not subject to unauthorized disclosure; or

b. The acquisition, distribution, or disclosure of, or access to, encrypted or redacted records or data without the accompanying acquisition of or reasonable ability to access or discover the confidential process or key necessary to unencrypt or decipher the records or data~~["Personally identifiable information" means an individual's first name or first initial and last name 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; or~~

~~3. Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account~~].

(2) Any information holder shall disclose any ***security*** breach~~[of the security of the system]~~, following discovery or notification of the breach~~[in the security of the~~

~~data]~~, to any resident of Kentucky whose ***personally identifiable*** ~~[unencrypted personal]~~ information was, or is reasonably believed to have been, ***subject to the security breach*** ~~[acquired by an unauthorized person]~~. The disclosure shall be made ***as soon as*** ~~[in the most expedient time]~~ possible and without unreasonable delay, 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]~~.

(3) Any information holder that maintains computerized data that includes personally identifiable information that the information holder does not own shall notify the owner or licensee of the information of any ***security*** breach ~~[of the security]~~ of the data as soon as reasonably practicable following discovery, if the personally identifiable information was, or is reasonably believed to have been, ***subject to the security breach*** ~~[acquired by an unauthorized person]~~.

(4) The notification required by this section may be delayed if a law enforcement agency 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) ***(a)*** For purposes of this section, notice may be provided by one (1) of the following methods:

1. ~~[(a)]~~ Written notice;

2. ~~[(b)]~~ 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; or

3. ~~[(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:

a. ~~[1.]~~ E-mail notice, when the information holder has an e-mail address for the subject persons;

b. ~~[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

c. ~~[3.]~~ Notification to major statewide media.

(b) Electronic or substitute notice shall not be provided to an e-mail or other electronic account if the security breach involved information that the information holder reasonably believes would or may permit an unauthorized person access to that account.

(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 ***security*** 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) ***An individual who has received notice of a security breach pursuant to subsection (2) of this section shall be entitled to three (3) copies of a consumer report from each nationwide consumer reporting agency, as defined in Section 1 of this Act,***

at no cost to the consumer. These three (3) consumer reports shall be in addition to any copies provided for under the Fair Credit Reporting Act, 15 U.S.C. secs. 1681 et seq., and shall have no time limitation within which they have to be requested by the individual.

(9) An individual shall not, as a condition of exercising his or her rights under any of the provisions of this section, be required to:

(a) Waive any right to a private right of action; or

(b) Agree to submit to a binding arbitration procedure.

(10) An information holder who owns or licenses the personally identifiable information of more than one thousand (1,000) residents of the Commonwealth of Kentucky shall encrypt, to the extent technologically feasible, all personally identifiable information transmitted or held by that information holder. If encryption is not technologically feasible, the information holder shall develop, implement, and maintain alternative compensating controls consistent with industry standards and the information holder's assessment of risk, to protect the security, confidentiality, and integrity of the personally identifiable information.

(11) Except as otherwise provided in Section 3 of this Act, the provisions of this section~~[and the requirements for nonaffiliated third parties in KRS Chapter 61]~~ shall not apply to***:***

(a) ~~[ ]~~Any person who is subject to the provisions of***:***

1. ~~[ ]~~Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended***;***~~[,]~~ or

2. ~~[ ]~~The ~~[federal]~~Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended***;***~~[, or]~~

(b) ~~[ ]~~Any agency of the Commonwealth of Kentucky or any of its local governments or political subdivisions***; or***

(c) A consumer reporting agency subject to Section 3 of this Act.

➔Section 6. 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) "***Encrypt***~~[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) ***(a)*** "Nonaffiliated third party" means any person that:

1. ~~[(a)]~~ Has a contract or agreement with an agency; and

2. ~~[(b)]~~ Receives ***personally identifiable*** ~~[personal]~~ information from the agency pursuant to the contract or agreement**.**

(b) "Nonaffiliated third party" does not include:

1. Any person who is subject to the provisions of:

a. Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended; or

b. The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, as amended; or

2. Any agency of the Commonwealth of Kentucky or any of its local governments or political subdivisions;

(6) "***Personally identifiable*** ~~[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 ***any*** 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 ***or without*** any ~~[required]~~security code, ***security question and answer,*** access code, or password ***that permits*** ~~[, would permit]~~ access to ***the*** ~~[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, ***or*** manipulation~~[, or release]~~ of***, or access to,***~~[unencrypted or unredacted]~~ records or data that***:***

1. Compromises***,*** or the agency or nonaffiliated third party reasonably believes may compromise***,*** the security, confidentiality, or integrity of ***personally identifiable***~~[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 ~~***Results***~~[result]~~ in the likelihood of harm to one (1) or more individuals.

(b) "Security breach" does not include***:***

1. The good-faith acquisition of ***or access to personally identifiable***~~[personal]~~ information by an employee, agent, or nonaffiliated third party of the agency~~[for the purposes of the agency]~~ if the ***personally identifiable***~~[personal]~~ information is used for a ***lawful*** purpose related to the agency and is not subject to unauthorized disclosure***; or***

2. The acquisition, distribution, or disclosure of, or access to, encrypted or redacted records or data without the accompanying acquisition of or reasonable ability to access or discover the confidential process or key necessary to unencrypt or decipher the records or data.

➔Section 7. KRS 61.932 is amended to read as follows:

(1) (a) An agency or nonaffiliated third party that maintains or otherwise possesses ***personally identifiable***~~[personal]~~ information, regardless of the form in which the ***personally identifiable***~~[personal]~~ information is maintained, shall implement, maintain, and update security procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches.

(b) Reasonable security and breach investigation procedures and practices established and implemented by organizational units of the executive branch of state government shall be in accordance with relevant enterprise policies established by the Commonwealth Office of Technology. Reasonable security and breach investigation procedures and practices established and implemented by units of government listed under KRS 61.931(1)(b) and (c) that are not organizational units of the executive branch of state government

shall be in accordance with policies established by the Department for Local Government. The Department for Local Government shall consult with public entities as defined in KRS 65.310 in the development of policies establishing reasonable security and breach investigation procedures and practices for units of local government pursuant to this subsection. Reasonable security and breach investigation procedures and practices established and implemented by public school districts listed under KRS 61.931(1)(d) shall be in accordance with administrative regulations promulgated by the Kentucky Board of Education. Reasonable security and breach investigation procedures and practices established and implemented by educational entities listed under KRS 61.931(1)(e) shall be in accordance with policies established by the Council on Postsecondary Education. The Commonwealth Office of Technology shall, upon request of an agency, make available technical assistance for the establishment and implementation of reasonable security and breach investigation procedures and practices.

(c) 1. If an agency is subject to any additional requirements under the Kentucky Revised Statutes or under federal law, protocols, or agreements relating to the protection and privacy of ***personally identifiable*** ~~[personal]~~ information, the agency shall comply with these additional requirements, in addition to the requirements of KRS 61.931 to 61.934.

2. If a nonaffiliated third party is required by federal law or regulation to conduct security breach investigations or to make notifications of security breaches, or both, as a result of the nonaffiliated third party's unauthorized disclosure of one (1) or more data elements of ***personally identifiable*** ~~[personal]~~ information that is the same as one (1) or more of the data elements of ***personally identifiable*** ~~[personal]~~ information listed

in KRS 61.931(6)(a) to (f), the nonaffiliated third party shall meet the requirements of KRS 61.931 to 61.934 by providing to the agency a copy of any and all reports and investigations relating to such security breach investigations or notifications that are required to be made by federal law or regulations. This subparagraph shall not apply if the security breach includes the unauthorized disclosure of data elements that are not covered by federal law or regulation but are listed in KRS 61.931(6)(a) to (f).

(2) (a) For agreements executed or amended on or after January 1, 2015, any agency that contracts with a nonaffiliated third party and that discloses ***personally identifiable*** ~~[personal]~~ information to the nonaffiliated third party shall require as part of that agreement that the nonaffiliated third party implement, maintain, and update security and breach investigation procedures that are appropriate to the nature of the information disclosed, that are at least as stringent as the security and breach investigation procedures and practices referenced in subsection (1)(b) of this section, and that are reasonably designed to protect the ***personally identifiable*** ~~[personal]~~ information from unauthorized access, use, modification, disclosure, manipulation, or destruction.

(b) 1. A nonaffiliated third party that is provided access to ***personally identifiable*** ~~[personal]~~ information by an agency, or that collects and maintains ***personally identifiable*** ~~[personal]~~ information on behalf of an agency shall notify the agency ***as soon as*** ~~[in the most expedient time]~~ possible and without unreasonable delay but within seventy-two (72) hours of determination of a security breach relating to the ***personally identifiable*** ~~[personal]~~ information in the possession of the nonaffiliated third party. The notice to the agency shall include all information the

nonaffiliated third party has with regard to the security breach at the time of notification. Agreements referenced in paragraph (a) of this subsection shall specify how the cost of the notification and investigation requirements under KRS 61.933 are to be apportioned when a security breach is suffered by the agency or nonaffiliated third party.

2. The notice required by subparagraph 1. of this paragraph may be delayed if a law enforcement agency notifies the nonaffiliated third party that notification will impede a criminal investigation or jeopardize homeland or national security. If notice is delayed pursuant to this subparagraph, notification shall be given as soon as reasonably feasible by the nonaffiliated third party to the agency with which the nonaffiliated third party is contracting. The agency shall then record the notification in writing on a form developed by the Commonwealth Office of Technology that the notification will not impede a criminal investigation and will not jeopardize homeland or national security. The Commonwealth Office of Technology shall promulgate administrative regulations under KRS 61.931 to 61.934 regarding the content of the form.

➔Section 8. KRS 61.933 is amended to read as follows:

(1) (a) Any agency that collects, maintains, or stores ***personally identifiable*** ~~[personal]~~ information that determines or is notified of a security breach relating to ***personally identifiable*** ~~[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 ***personally identifiable***~~[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 ***personally identifiable***~~[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 ***personally identifiable*** ~~[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 ***personally identifiable*** ~~[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 ***e-mail*** ~~[electronic mail]~~, sent to the most recent ***e-mail*** ~~[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 ***he or she does*** ~~[they do]~~ not want ***e-mail*** ~~[email]~~ notification ***or the security breach involved information that the agency or nonaffiliated third party reasonably believes would permit an unauthorized person access to the e-mail account***; 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 ***personally identifiable*** ~~[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 ***personally identifiable*** ~~[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) ***Personally identifiable***~~[personal]~~ information***:***

1. That has been redacted;

2.~~[(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;

3.~~[(c)]~~ ~~[Personal information]~~That is publicly and lawfully made available to the general public from federal, state, or local government records; ***or***

4.~~[(d)]~~ ~~[Personal information]~~That an individual has consented to have

publicly disseminated or listed; or

(b)~~[(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) 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.

➔Section 9. KRS 61.934 is amended to read as follows:

(1) The legislative and judicial branches of state government shall implement, maintain, and update reasonable security and breach investigation procedures and practices, including taking any appropriate corrective action, to protect and safeguard against security breaches consistent with KRS 61.931 to 61.934.

(2) The Department for Libraries and Archives shall establish procedures for the appropriate disposal or destruction of records that include ***personally identifiable***~~[personal]~~ information pursuant to the authority granted the Department for Libraries and Archives under KRS 171.450.

➔Section 10. KRS 171.450 is amended to read as follows:

(1) The department shall establish:

(a) Procedures for the compilation and submission to the department of lists and schedules of public records proposed for disposal;

(b) Procedures for the disposal or destruction of public records authorized for disposal or destruction, including appropriate procedures to protect against unauthorized access to or use of ***personally identifiable***~~[personal]~~ information as defined by KRS 61.931;

(c) Standards and procedures for recording, managing, and preserving public records and for the reproduction of public records by photographic or

microphotographic process; and

(d) Procedures for collection and distribution by the central depository of all reports and publications, except the Kentucky Revised Statutes editions, issued by any department, board, commission, officer or other agency of the Commonwealth for general public distribution after July 1, 1958.

(2) The department shall enforce the provisions of KRS 171.410 to 171.740 by appropriate rules and regulations.

(3) The department shall make copies of such rules and regulations available to all officials affected by KRS 171.410 to 171.740 subject to the provisions of KRS Chapter 13A.

(4) Such rules and regulations when approved by the department shall be binding on all state and local agencies, subject to the provisions of KRS Chapter 13A. The department shall perform any acts deemed necessary, legal and proper to carry out the duties and responsibilities imposed upon it pursuant to the authority granted herein.

➔Section 11. KRS 42.722 is amended to read as follows:

As used in KRS 42.720 to 42.742:

(1) "Communications" or "telecommunications" means any transmission, emission, or reception of signs, signals, writings, images, and sounds of intelligence of any nature by wire, radio, optical, or other electromagnetic systems, and includes all facilities and equipment performing these functions;

(2) "Geographic information system" or "GIS" means a computerized database management system for the capture, storage, retrieval, analysis, and display of spatial or locationally defined data;

(3) "Information resources" means the procedures, equipment, and software that are designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel;

(4) "Information technology" means data processing and telecommunications hardware, software, services, supplies, facilities, maintenance, and training that are used to support information processing and telecommunications systems to include geographic information systems;

(5) "***Personally identifiable***~~[personal]~~ information " has the same meaning as in KRS 61.931;

(6) "Project" means a program to provide information technologies support to functions within an executive branch state agency, which should be characterized by well-defined parameters, specific objectives, common benefits, planned activities, expected outcomes and completion dates, and an established budget with a specified source of funding;

(7) "Security breach" has the same meaning as in KRS 61.931; and

(8) "Technology infrastructure" means any computing equipment, servers, networks, storage, desktop support, telephony, enterprise shared systems, information technology security, disaster recovery, business continuity, database administration, and software licensing.

➔Section 12. KRS 42.726 is amended to read as follows:

(1) The roles and duties of the Commonwealth Office of Technology shall include but not be limited to:

(a) Providing technical support and services to all executive agencies of state government in the application of information technology;

(b) Assuring compatibility and connectivity of Kentucky's information systems;

(c) Developing strategies and policies to support and promote the effective applications of information technology within state government as a means of saving money, increasing employee productivity, and improving state services to the public, including electronic public access to information of the Commonwealth;

(d) Developing, implementing, and managing strategic information technology directions, standards, and enterprise architecture, including implementing necessary management processes to assure full compliance with those directions, standards, and architecture;

(e) Promoting effective and efficient design and operation of all major information resources management processes for executive branch agencies, including improvements to work processes;

(f) Developing, implementing, and maintaining the technology infrastructure of the Commonwealth and all related support staff, planning, administration, asset management, and procurement for all executive branch cabinets and agencies except:

1. Agencies led by a statewide elected official;
2. The nine (9) public institutions of postsecondary education;
3. The Department of Education's services provided to local school districts;
4. The Kentucky Retirement Systems and the Teachers' Retirement System;
5. The Kentucky Housing Corporation;
6. The Kentucky Lottery Corporation;
7. The Kentucky Higher Education Student Loan Corporation; and
8. The Kentucky Higher Education Assistance Authority;

(g) Facilitating and fostering applied research in emerging technologies that offer the Commonwealth innovative business solutions;

(h) Reviewing and overseeing large or complex information technology projects and systems for compliance with statewide strategies, policies, and standards, including alignment with the Commonwealth's business goals, investment, and other risk management policies. The executive director is authorized to

grant or withhold approval to initiate these projects;

(i) Integrating information technology resources to provide effective and supportable information technology applications in the Commonwealth;

(j) Establishing a central statewide geographic information clearinghouse to maintain map inventories, information on current and planned geographic information systems applications, information on grants available for the acquisition or enhancement of geographic information resources, and a directory of geographic information resources available within the state or from the federal government;

(k) Coordinating multiagency information technology projects, including overseeing the development and maintenance of statewide base maps and geographic information systems;

(l) Providing access to both consulting and technical assistance, and education and training, on the application and use of information technologies to state and local agencies;

(m) In cooperation with other agencies, evaluating, participating in pilot studies, and making recommendations on information technology hardware and software;

(n) Providing staff support and technical assistance to the Geographic Information Advisory Council and the Kentucky Information Technology Advisory Council;

(o) Overseeing the development of a statewide geographic information plan with input from the Geographic Information Advisory Council;

(p) Developing for state executive branch agencies a coordinated security framework and model governance structure relating to the privacy and confidentiality of ***personally identifiable*** ~~[personal]~~ information collected and stored by state executive branch agencies, including but not limited to:

1. Identification of key infrastructure components and how to secure them;
2. Establishment of a common benchmark that measures the effectiveness of security, including continuous monitoring and automation of defenses;
3. Implementation of vulnerability scanning and other security assessments;
4. Provision of training, orientation programs, and other communications that increase awareness of the importance of security among agency employees responsible for ***personally identifiable*** ~~[personal]~~ information; and
5. Development of and making available a cyber security incident response plan and procedure; and

(q) Preparing proposed legislation and funding proposals for the General Assembly that will further solidify coordination and expedite implementation of information technology systems.

(2) The Commonwealth Office of Technology may:

(a) Provide general consulting services, technical training, and support for generic software applications, upon request from a local government, if the executive director finds that the requested services can be rendered within the established terms of the federally approved cost allocation plan;

(b) Promulgate administrative regulations in accordance with KRS Chapter 13A necessary for the implementation of KRS 42.720 to 42.742, 45.253, 171.420, 186A.040, 186A.285, and 194A.146;

(c) Solicit, receive, and consider proposals from any state agency, federal agency, local government, university, nonprofit organization, private person, or corporation;

(d) Solicit and accept money by grant, gift, donation, bequest, legislative

appropriation, or other conveyance to be held, used, and applied in accordance with KRS 42.720 to 42.742, 45.253, 171.420, 186A.040, 186A.285, and 194A.146;

(e) Make and enter into memoranda of agreement and contracts necessary or incidental to the performance of duties and execution of its powers, including, but not limited to, agreements or contracts with the United States, other state agencies, and any governmental subdivision of the Commonwealth;

(f) Accept grants from the United States government and its agencies and instrumentalities, and from any source, other than any person, firm, or corporation, or any director, officer, or agent thereof that manufactures or sells information resources technology equipment, goods, or services. To these ends, the Commonwealth Office of Technology shall have the power to comply with those conditions and execute those agreements that are necessary, convenient, or desirable; and

(g) Purchase interest in contractual services, rentals of all types, supplies, materials, equipment, and other services to be used in the research and development of beneficial applications of information resources technologies. Competitive bids may not be required for:

1. New and emerging technologies as approved by the executive director or her or his designee; or

2. Related professional, technical, or scientific services, but contracts shall be submitted in accordance with KRS 45A.690 to 45A.725.

(3) Nothing in this section shall be construed to alter or diminish the provisions of KRS 171.410 to 171.740 or the authority conveyed by these statutes to the Archives and Records Commission and the Department for Libraries and Archives.

(4) The Commonwealth Office of Technology shall, on or before October 1 of each year, submit to the Legislative Research Commission a report in accordance with

KRS 57.390 detailing:

(a) Any security breaches that occurred within organizational units of the executive branch of state government during the prior fiscal year that required notification to the Commonwealth Office of Technology under KRS 61.932;

(b) Actions taken to resolve the security breach, and to prevent additional security breaches in the future;

(c) A general description of what actions are taken as a matter of course to protect personal data from security breaches; and

(d) Any quantifiable financial impact to the agency reporting a security breach.

➔Section 13. Whereas consumer reporting agencies maintain sensitive identifying information of millions of consumers and play a critical role in the consumer financial services marketplace, and the prevalence of security breaches containing sensitive identifying information of consumers is on the rise, as is the accompanying risk of identity theft for those consumers exposed as a result of these breaches, an emergency is declared to exist, and this Act takes effect upon its passage and approval by the Governor or upon its otherwise becoming a law.