

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

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

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

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

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

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

11 ~~(3)(2)~~ "Consumer report" means a consumer report, as defined in the ~~federal~~ Fair  
12 Credit Reporting Act, 15 U.S.C. sec. 1681a(d);

13 ~~(4)(3)~~ "Consumer reporting agency" means a consumer reporting agency as defined  
14 by the ~~federal~~ Fair Credit Reporting Act, 15 U.S.C. sec. 1681a(f). "Consumer  
15 reporting agency" shall not mean a check acceptance service which provides check  
16 approval and guarantees services to merchants;~~and~~

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

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

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

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

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

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

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

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

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

10 (b) A Social Security number;

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

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

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

16 (f) Individually identifiable health information as defined in 45 C.F.R. sec.  
17 160.103;

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

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

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

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

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

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

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

7 ~~(10)~~(4) "Security freeze" means a notice placed on a consumer file, at the request of  
 8 the consumer and subject to certain exceptions, that prohibits a consumer reporting  
 9 agency from releasing the consumer's consumer report or credit score relating to the  
 10 extension of credit without the express authorization of the consumer; and

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

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

15 (1) For the purposes of this section:

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

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

- 21 1. Identifies a protected person;
- 22 2. Is created by a consumer reporting agency solely for the purpose of  
 23 complying with this section; and
- 24 3. Is not created or used to consider the protected person's  
 25 creditworthiness, credit standing, credit capacity, character, general  
 26 reputation, personal characteristics, or mode of living;

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

- 1 agency sufficient proof of authority to act on behalf of a protected person; and
- 2 (d) "Sufficient proof of authority" means documentation that shows a
- 3 representative has authority to act on behalf of a protected person, including
- 4 but not limited to:
- 5 1. A court order granting custodianship, guardianship, or conservatorship;
  - 6 2. A birth certificate;
  - 7 3. A lawfully executed and valid power of attorney; or
  - 8 4. A written, notarized statement signed by a representative that expressly
  - 9 describes the authority of the representative to act on behalf of a
  - 10 protected person.
- 11 (2) A consumer reporting agency shall place a security freeze on a protected person's
- 12 record or consumer~~credit~~ report if:
- 13 (a) The consumer reporting agency receives a request from the protected person's
  - 14 representative for the placement of the security freeze; and
  - 15 (b) The protected person's representative:
    - 16 1. Submits the request to the consumer reporting agency ***using the method***
    - 17 ***that the agency has established to receive security freeze requests***~~at~~
    - 18 ~~the address designated by the consumer reporting agency to receive the~~
    - 19 ~~request~~;
    - 20 2. Provides to the consumer reporting agency clear and proper
    - 21 identification of the protected person and the representative;
    - 22 3. Provides to the consumer reporting agency sufficient proof of authority
    - 23 to act on behalf of the protected person; and
    - 24 4. Pays to the consumer reporting agency a fee as prescribed in subsection
    - 25 (8) of this section.
- 26 (3) If a consumer reporting agency does not have a file pertaining to a protected person
- 27 when the consumer reporting agency receives a request pursuant to subsection (2) of

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

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

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

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

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

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

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

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

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

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

- 1           2. If the protected person's representative requested the removal of the  
2 security freeze on behalf of the protected person, the protected person's  
3 representative shall provide to the consumer reporting agency both of  
4 the following:
- 5           a. Clear and proper identification of the protected person and the  
6 representative; and
- 7           b. Sufficient proof of authority to act on behalf of the protected  
8 person.
- 9           (b) Within thirty (30) days after receiving a request to remove a security freeze  
10 placed pursuant to subsection (2) of this section, the consumer reporting  
11 agency shall remove the security freeze for the protected person.
- 12 (8) A consumer reporting agency may charge a fee for each placement or removal of a  
13 security freeze on a protected person's record or consumer~~credit~~ report. The fee  
14 ~~shall~~~~may~~ not exceed ten dollars (\$10).
- 15 (9) Notwithstanding subsection (8) of this section, a consumer reporting agency  
16 ~~shall~~~~may~~ not charge a~~any~~ fee under this section if:
- 17           (a) The protected **person or the protected person's representative has received a**  
18 **notification of a security breach pursuant to Section 3, 5, or 8 of this Act**  
19 **that affects the protected person and, upon request, provides a copy of the**  
20 **notification to the consumer reporting agency;**
- 21           **(b) The protected person is a victim of identity theft and, upon request, the**  
22 **protected person or the protected** person's representative provides a copy of a  
23 **valid** police report to the consumer reporting agency~~—alleging that the~~  
24 ~~protected person has been a victim of an offense involving identity theft;~~~~—or~~
- 25 ~~(c)~~~~(b)~~ A request for the placement or removal of a security freeze is for a  
26 protected person who is under sixteen (16) years of age at the time of the  
27 request and the consumer reporting agency has a consumer~~credit~~ report

1           pertaining to the protected person; or

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

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

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

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

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

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

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

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

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

1 record provided to:

- 2 (a) A federal, state, or local governmental entity, including a law enforcement  
3 agency, or court, or their agents or assigns;
- 4 (b) A private collection agency for the sole purpose of assisting in the collection  
5 of an existing debt of the consumer who is the subject of the consumer report  
6 requested;
- 7 (c) A person or entity, or a subsidiary, affiliate, or agent of that person or entity,  
8 or an assignee of a financial obligation owing by the consumer to that person  
9 or entity, or a prospective assignee of a financial obligation owing by the  
10 consumer to that person or entity in conjunction with the proposed purchase of  
11 the financial obligation, with which the consumer has or had prior to  
12 assignment an account or contract, including a demand deposit account, or to  
13 whom the consumer issued a negotiable instrument, for the purposes of  
14 reviewing the account or collecting the financial obligation owing for the  
15 account, contract, or negotiable instrument. For purposes of this paragraph,  
16 "reviewing the account" includes activities related to account maintenance,  
17 monitoring, credit line increases, and account upgrades and enhancements;
- 18 (d) A person~~[,]~~ for the purposes of prescreening as provided by the~~[ federal]~~ Fair  
19 Credit Reporting Act, 15 U.S.C. secs. 1681 et seq.;
- 20 (e) A consumer reporting agency for the purposes of providing a consumer with a  
21 copy of his or her own report on the consumer's~~[his or her]~~ request;
- 22 (f) A child support enforcement agency;
- 23 (g) A consumer reporting agency that acts only as a reseller of credit information  
24 by assembling and merging information contained in the database of another  
25 consumer reporting agency or multiple credit reporting agencies and does not  
26 maintain a permanent database of credit information from which new  
27 consumer reports are produced. However, a consumer reporting agency acting



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

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

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

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

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

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

- 18 a. Criminal record information;
- 19 b. Personal loss history information;
- 20 c. Fraud prevention or detection;
- 21 d. Employment screening; or
- 22 e. Tenant screening.

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

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

25 **(a) The consumer file of a consumer; and**

26 **(b) Each consumer report of a consumer both:**

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

1 third-party agent; and

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

4 ~~(2)~~~~(1)~~ (a) A consumer may elect to place a security freeze on the consumer's  
 5 consumer report by written request~~[, sent by certified mail, that includes clear~~  
 6 ~~and proper identification.]~~ to a consumer reporting agency at an address  
 7 designated by the consumer reporting agency to receive security freeze  
 8 requests, or by the use of telephone, fax, or Web-based or other electronic  
 9 method that the consumer reporting agency has established to receive  
 10 security freeze requests. A request made pursuant to this subsection shall  
 11 include clear and proper identification~~[such request].~~ A consumer reporting  
 12 agency shall place a security freeze on a consumer's consumer report no later  
 13 than ten (10) business days after receiving a ~~written~~ request made pursuant  
 14 to this subsection for the placement of a security freeze from the consumer.

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

20 ~~(3)~~~~(2)~~ The consumer reporting agency shall, no later than ten (10) business days after  
 21 the date the agency receives the request for a security freeze, provide the consumer  
 22 with a unique personal identification number or password to be used by the  
 23 consumer when providing authorization for the access to his or her credit file for a  
 24 specific period of time. In addition, the consumer reporting agency shall  
 25 simultaneously provide to the consumer in writing the process of placing, removing,  
 26 and temporarily lifting a security freeze and the process for allowing access to  
 27 information from the consumer's credit file for a specific period while the security

1 freeze is in effect.

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

14 ~~(5)~~~~(4)~~ If a third party requests access to a consumer report on which a security freeze  
15 is in effect, and this request is in connection with an application for credit, the third  
16 party may treat the application as incomplete.

17 ~~(6)~~~~(5)~~ If the consumer wishes to allow his **or her** consumer report or credit score to  
18 be accessed for a specific period of time while a freeze is in place, the consumer  
19 shall contact the consumer reporting agency and request that the freeze be  
20 temporarily lifted and provide the following:

- 21 (a) Clear and proper identification;
- 22 (b) The unique personal identification number or password provided by the  
23 consumer reporting agency pursuant to subsection ~~[(2) or ]~~(3) **or (4)** of this  
24 section; and
- 25 (c) The proper information regarding the time period for which the report shall be  
26 available to users of the consumer report.

27 ~~(7)~~~~(6)~~ A consumer reporting agency that receives a request from a consumer to

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

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

- 10 (a) Upon the consumer's~~consumer~~ request made pursuant to subsection (6) or  
 11 (9)~~of~~~~as provided in~~ this section; or  
 12 (b) If the~~consumer's~~ consumer report was frozen due to a material  
 13 misrepresentation of fact by the consumer. If a consumer reporting agency  
 14 intends to remove a freeze upon a~~consumer's~~ consumer report pursuant to  
 15 this paragraph, the consumer reporting agency shall notify the consumer in  
 16 writing prior to removing the freeze on the~~consumer's~~ consumer report.

17 ~~(9)~~~~(8)~~ A security freeze shall remain in place until the consumer requests that the  
 18 security freeze be removed, or the consumer reporting agency has notified the  
 19 consumer in writing that it is removing the freeze due to a misrepresentation of  
 20 fact by the consumer pursuant to subsection (8)(b) of this section~~but no longer~~  
 21 ~~than seven (7) years from the date the security freeze was put in place~~. A consumer  
 22 reporting agency shall remove a security freeze within three (3) business days of  
 23 receiving:

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

25 (b) Both of the following:

26 1.~~(a)~~ Clear and proper identification; and

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

1 by the consumer reporting agency.

2 ~~(10)~~~~(9)~~ A security freeze does not apply to a consumer report provided to:

- 3 (a) A federal, state, or local governmental entity, including a law enforcement  
4 agency, or court, or their agents or assigns;
- 5 (b) A private collection agency for the sole purpose of assisting in the collection  
6 of an existing debt of the consumer who is the subject of the consumer report  
7 requested;
- 8 (c) A person or entity, or a subsidiary, affiliate, or agent of that person or entity,  
9 or an assignee of a financial obligation owing by the consumer to that person  
10 or entity, or a prospective assignee of a financial obligation owing by the  
11 consumer to that person or entity in conjunction with the proposed purchase of  
12 the financial obligation, with which the consumer has or had prior to  
13 assignment an account or contract, including a demand deposit account, or to  
14 whom the consumer issued a negotiable instrument, for the purposes of  
15 reviewing the account or collecting the financial obligation owing for the  
16 account, contract, or negotiable instrument. For purposes of this paragraph,  
17 "reviewing the account" includes activities related to account maintenance,  
18 monitoring, credit line increases, and account upgrades and enhancements;
- 19 (d) A subsidiary, affiliate, agent, assignee, or prospective assignee of a person to  
20 whom access has been granted under subsection ~~(6)~~~~(5)~~ of this section for the  
21 purposes of facilitating the extension of credit;
- 22 (e) A person~~,~~ for the purposes of prescreening as provided by the ~~federal~~ Fair  
23 Credit Reporting Act, 15 U.S.C. secs. 1681 et seq.;
- 24 (f) A consumer reporting agency for the purposes of providing a consumer with a  
25 copy of his or her own report on the consumer's~~his~~ request;
- 26 (g) A child support enforcement agency;
- 27 (h) A consumer reporting agency that acts only as a reseller of credit information

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

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

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

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

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

20 (11)~~[(10)]~~ A consumer reporting agency may impose a reasonable charge on a consumer  
21 for initially placing, temporarily lifting, or removing a security freeze on a consumer  
22 file. The amount of the charge may not exceed ten dollars (\$10). On January 1 of  
23 each year, a consumer reporting agency may increase the charge for placing a  
24 security freeze~~[alert]~~. The increase shall be based proportionally on changes to the  
25 Consumer Price Index for All Urban Consumers as determined by the United States  
26 Department of Labor with fractional changes rounded to the nearest twenty-five  
27 cents (\$0.25).~~[An exception shall be allowed whereby the consumer will be~~

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

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

5 **(a)** The consumer:

6 **1. Has received a notification:**

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

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

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

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

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

20 **1.[(a)]** Name;

21 **2.[(b)]** Date of birth;

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

23 **4.[(d)]** Address.

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

1 and to the former address.

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

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

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

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

10 **2. Reimburse the consumer for credit monitoring purchased by the**  
11 **consumer.**

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

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

23 **(17) A consumer reporting agency shall comply with subsections (3) and (9) of Section**  
24 **5 of this Act.**

25 **(18)**~~(12)~~ Any person who willfully fails to comply with any requirement imposed under  
26 this section with respect to any consumer is liable to that consumer in an amount  
27 equal to the sum of:



- 1 (a) Any actual damages sustained by the consumer as a result of the failure;
- 2 (b) Any liquidated damages of not less than one hundred dollars (\$100) and not
- 3 more than one thousand dollars (\$1,000);
- 4 (c) Any punitive damages as the court may allow; and
- 5 (d) In the case of any successful action to enforce any liability under this section,
- 6 the costs of the action together with reasonable attorney's fees as determined
- 7 by the court.

8 ~~(19)~~~~(13)~~ Any person, other than the named individual or individuals in the report, who

9 obtains a consumer report, requests a security freeze, requests the temporary lift of a

10 freeze, or the removal of a security freeze from a consumer reporting agency under

11 false pretenses or in an attempt to violate federal or state law shall be liable to the

12 consumer reporting agency for actual damages sustained by the consumer reporting

13 agency or one thousand dollars (\$1,000), whichever is greater.

14 ~~(20)~~~~(14)~~ Any person who is negligent in failing to comply with any requirement

15 imposed under this section with respect to any consumer is liable to that consumer

16 in an amount equal to the sum of:

- 17 (a) Any actual damages sustained by the consumer as a result of the failure; and
- 18 (b) In the case of any successful action to enforce any liability under this section,
- 19 the costs of the action together with reasonable attorney's fees as determined
- 20 by the court.

21 **(21) An individual shall not, as a condition of exercising his or her rights under any**

22 **of the provisions of this section, be required to:**

- 23 **(a) Waive any right to a private right of action; or**
- 24 **(b) Agree to submit to a binding arbitration procedure.**

25 ~~(22)~~~~(15)~~ Nothing in KRS 367.363 to 367.365 shall be construed to limit or restrict the

26 exercise of powers or the performance of the duties of the Attorney General

27 authorized under any other provision of law to bring or seek redress for persons that

1 violate KRS 367.363 to 367.365.

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

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

- 4 (1) "Business" means a sole proprietorship, partnership, corporation, limited liability  
5 company, association, or other entity, however organized and whether or not  
6 organized to operate at a profit. "Business" shall not mean a bank as defined in 12  
7 U.S.C. sec. 1813(a) or Subtitles 1, 2, and 3 of KRS Chapter 286, a credit union as  
8 defined in 12 U.S.C. sec. 1752 or Subtitle 6 of KRS Chapter 286, a savings  
9 association as defined in 12 U.S.C. sec. 1813(b), or an association as defined in  
10 Subtitle 5 of KRS Chapter 286. The term includes an entity that destroys records;
- 11 (2) "Customer" means an individual who provides personally identifiable~~[personal]~~  
12 information to a business for the purpose of purchasing or leasing a product or  
13 obtaining a service for business;
- 14 (3) "Individual" means a natural person;
- 15 (4) "Personally identifiable information" means an individual's first name or first  
16 initial and last name, personal mark, or unique biometric or genetic print or  
17 image, in combination with any one (1) or more of the following data elements:
- 18 (a) An account number, credit card number, debit card number, user name, or  
19 e-mail address with or without any security code, security question and  
20 answer, access code, or password that permits access to an individual's  
21 account;
- 22 (b) A Social Security number;
- 23 (c) A tax identification number that incorporates a Social Security number;
- 24 (d) A driver's license number, state identification card number, or other  
25 identification number issued by a state;
- 26 (e) A passport number or other identification number issued by the United  
27 States government; or

1 (f) *Individually identifiable health information as defined in 45 C.F.R. sec.*

2 160.103~~[means data capable of being associated with a particular customer~~  
 3 ~~through one (1) or more identifiers, including but not limited to a customer's~~  
 4 ~~name, address, telephone number, electronic mail address, fingerprints,~~  
 5 ~~photographs or computerized image, Social Security number, passport~~  
 6 ~~number, driver identification number, personal identification card number or~~  
 7 ~~code, date of birth, medical information, financial information, tax~~  
 8 ~~information, and disability information]; and~~

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

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

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

14 (a) "Encrypt" has the same meaning as in Section 6 of this Act~~["Breach of the~~  
 15 ~~security of the system" means unauthorized acquisition of unencrypted and~~  
 16 ~~unredacted computerized data that compromises the security, confidentiality,~~  
 17 ~~or integrity of personally identifiable information maintained by the~~  
 18 ~~information holder as part of a database regarding multiple individuals that~~  
 19 ~~actually causes, or leads the information holder to reasonably believe has~~  
 20 ~~caused or will cause, identity theft or fraud against any resident of the~~  
 21 ~~Commonwealth of Kentucky. Good faith acquisition of personally identifiable~~  
 22 ~~information by an employee or agent of the information holder for the~~  
 23 ~~purposes of the information holder is not a breach of the security of the system~~  
 24 ~~if the personally identifiable information is not used or subject to further~~  
 25 ~~unauthorized disclosure];~~

- 26 (b) "Information holder" means any person or business entity that conducts  
 27 business in this state; and

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

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

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

8 2. "Security breach" does not include:

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

13 b. The acquisition, distribution, or disclosure of, or access to,  
 14 encrypted or redacted records or data without the accompanying  
 15 acquisition of or reasonable ability to access or discover the  
 16 confidential process or key necessary to unencrypt or decipher  
 17 the records or data["Personally identifiable information" means an

18 individual's first name or first initial and last name in combination  
 19 with any one (1) or more of the following data elements, when the  
 20 name or data element is not redacted:

21 1. Social Security number;

22 2. Driver's license number; or

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

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

1       ~~data~~, to any resident of Kentucky whose personally identifiable~~unencrypted~~  
2       ~~personal~~ information was, or is reasonably believed to have been, subject to the  
3       security breach~~acquired by an unauthorized person~~. The disclosure shall be made  
4       as soon as~~in the most expedient time~~ possible and without unreasonable delay,  
5       consistent with the legitimate needs of law enforcement, as provided in subsection  
6       (4) of this section, or any measures necessary to determine the scope of the breach  
7       and restore the reasonable integrity of the data~~system~~.

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

14       (4) The notification required by this section may be delayed if a law enforcement  
15       agency determines that the notification will impede a criminal investigation. The  
16       notification required by this section shall be made promptly after the law  
17       enforcement agency determines that it will not compromise the investigation.

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

20               1.~~(a)~~       Written notice;

21               2.~~(b)~~       Electronic notice, if the notice provided is consistent with the  
22               provisions regarding electronic records and signatures set forth in 15  
23               U.S.C. sec. 7001; or

24               3.~~(c)~~       Substitute notice, if the information holder demonstrates that the  
25               cost of providing notice would exceed two hundred fifty thousand  
26               dollars (\$250,000), or that the affected class of subject persons to be  
27               notified exceeds five hundred thousand (500,000), or the information

1 holder does not have sufficient contact information. Substitute notice  
2 shall consist of all of the following:

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

5 b.~~[2.]~~ Conspicuous posting of the notice on the information holder's  
6 Internet Web site page, if the information holder maintains a Web  
7 site page; and

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

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

13 (6) Notwithstanding subsection (5) of this section, an information holder that maintains  
14 its own notification procedures as part of an information security policy for the  
15 treatment of personally identifiable information, and is otherwise consistent with  
16 the timing requirements of this section, shall be deemed to be in compliance with  
17 the notification requirements of this section, if it notifies subject persons in  
18 accordance with its policies in the event of a **security** breach~~[of security of the~~  
19 ~~system]~~.

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

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

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

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

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

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

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

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

20 (a) ~~Any person who is subject to the provisions of:~~

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

23 2. ~~The federal Health Insurance Portability and Accountability Act of~~  
 24 1996, Pub. L. No. 104-191, as amended; ~~or~~

25 (b) ~~Any agency of the Commonwealth of Kentucky or any of its local~~  
 26 governments or political subdivisions; or

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

1           ➔Section 6. KRS 61.931 is amended to read as follows:

2   As used in KRS 61.931 to 61.934:

3   (1) "Agency" means:

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

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

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

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

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

19   (2) "Commonwealth Office of Technology" means the office established by KRS  
20       42.724;

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

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

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

26   (4) "Law enforcement agency" means any lawfully organized investigative agency,  
27       sheriff's office, police unit, or police force of federal, state, county, urban-county



1 government, charter county, city, consolidated local government, unified local  
 2 government, or any combination of these entities, responsible for the detection of  
 3 crime and the enforcement of the general criminal federal and state laws;

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

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

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

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

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

10 **a. Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-**  
 11 **102, as amended; or**

12 **b. The Health Insurance Portability and Accountability Act of**  
 13 **1996, Pub. L. No. 104-191, as amended; or**

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

16 (6) **"Personally identifiable**~~[Personal]~~ information" means an individual's first name or  
 17 first initial and last name~~[,;-]~~ personal mark~~[,;-]~~ or unique biometric or genetic print  
 18 or image, in combination with **any** one (1) or more of the following data elements:

19 (a) An account number, credit card number,~~[-or]~~ debit card number, **user name,**  
 20 **or e-mail address** ~~[that, In combination]~~ with **or without** any ~~[required~~  
 21 ~~]security code, **security question and answer,** access code, or password **that**  
 22 **permits**~~[, would permit]~~ access to **the**~~[an]~~ account;~~

23 (b) A Social Security number;

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

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

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

1 government; or

2 (f) Individually identifiable health information as defined in 45 C.F.R. sec.  
3 160.103, except for education records covered by the Family Educational  
4 Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g;

5 (7) (a) "Public record or record," as established by KRS 171.410, means all books,  
6 papers, maps, photographs, cards, tapes, disks, diskettes, recordings, and other  
7 documentary materials, regardless of physical form or characteristics, which  
8 are prepared, owned, used, in the possession of, or retained by a public  
9 agency.

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

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

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

17 ~~1. —~~ the unauthorized acquisition, distribution, disclosure, destruction, or  
18 manipulation~~[, or release]~~ of, or access to,~~[unencrypted or unredacted]~~  
19 records or data that:

20 1. Compromises~~;~~ or the agency or nonaffiliated third party reasonably  
21 believes may compromise~~;~~ the security, confidentiality, or integrity of  
22 personally identifiable~~[personal]~~ information; and~~[result in the~~  
23 ~~likelihood of harm to one (1) or more individuals; or]~~

24 ~~2. [The unauthorized acquisition, distribution, disclosure, destruction,~~  
25 ~~manipulation, or release of encrypted records or data containing personal~~  
26 ~~information along with the confidential process or key to unencrypt the~~  
27 ~~records or data that compromises or the agency or nonaffiliated third~~

1           ~~party reasonably believes may compromise the security, confidentiality,~~  
 2           ~~or integrity of personal information and ]Results[result] in the likelihood~~  
 3           of harm to one (1) or more individuals.

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

- 5           1. The good-faith acquisition of or access to personally identifiable~~[~~  
 6           ~~personal]~~ information by an employee, agent, or nonaffiliated third party  
 7           of the agency~~[ for the purposes of the agency]~~ if the personally  
 8           identifiable~~[personal]~~ information is used for a lawful purpose related to  
 9           the agency and is not subject to unauthorized disclosure; or
- 10          2. The acquisition, distribution, or disclosure of, or access to, encrypted  
 11          or redacted records or data without the accompanying acquisition of  
 12          or reasonable ability to access or discover the confidential process or  
 13          key necessary to unencrypt or decipher the records or data.

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

- 15       (1) (a) An agency or nonaffiliated third party that maintains or otherwise possesses  
 16       personally identifiable~~[personal]~~ information, regardless of the form in which  
 17       the personally identifiable~~[personal]~~ information is maintained, shall  
 18       implement, maintain, and update security procedures and practices, including  
 19       taking any appropriate corrective action, to protect and safeguard against  
 20       security breaches.
- 21       (b) Reasonable security and breach investigation procedures and practices  
 22       established and implemented by organizational units of the executive branch  
 23       of state government shall be in accordance with relevant enterprise policies  
 24       established by the Commonwealth Office of Technology. Reasonable security  
 25       and breach investigation procedures and practices established and  
 26       implemented by units of government listed under KRS 61.931(1)(b) and (c)  
 27       that are not organizational units of the executive branch of state government

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

- 16 (c) 1. If an agency is subject to any additional requirements under the  
 17 Kentucky Revised Statutes or under federal law, protocols, or  
 18 agreements relating to the protection and privacy of **personally**  
 19 **identifiable**~~[personal]~~ information, the agency shall comply with these  
 20 additional requirements, in addition to the requirements of KRS 61.931  
 21 to 61.934.
- 22 2. If a nonaffiliated third party is required by federal law or regulation to  
 23 conduct security breach investigations or to make notifications of  
 24 security breaches, or both, as a result of the nonaffiliated third party's  
 25 unauthorized disclosure of one (1) or more data elements of **personally**  
 26 **identifiable**~~[personal]~~ information that is the same as one (1) or more of  
 27 the data elements of **personally identifiable**~~[personal]~~ information listed

1 in KRS 61.931(6)(a) to (f), the nonaffiliated third party shall meet the  
2 requirements of KRS 61.931 to 61.934 by providing to the agency a  
3 copy of any and all reports and investigations relating to such security  
4 breach investigations or notifications that are required to be made by  
5 federal law or regulations. This subparagraph shall not apply if the  
6 security breach includes the unauthorized disclosure of data elements  
7 that are not covered by federal law or regulation but are listed in KRS  
8 61.931(6)(a) to (f).

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

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

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

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

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

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

27 1. Notify the commissioner of the Kentucky State Police, the Auditor of

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

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

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

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

25 a. Within forty-eight (48) hours of completion of the investigation,  
26 notify in writing all officers listed in paragraph (a)1. of this  
27 subsection, and the commissioner of the Department for Libraries

- 1 and Archives, unless the provisions of subsection (3) of this
- 2 section apply;
- 3 b. Within thirty-five (35) days of providing the notifications required
- 4 by subdivision a. of this subparagraph, notify all individuals
- 5 impacted by the security breach as provided in subsection (2) of
- 6 this section, unless the provisions of subsection (3) of this section
- 7 apply; and
- 8 c. If the number of individuals to be notified exceeds one thousand
- 9 (1,000), the agency shall notify, at least seven (7) days prior to
- 10 providing notice to individuals under subdivision b. of this
- 11 subparagraph, the Commonwealth Office of Technology if the
- 12 agency is an organizational unit of the executive branch of state
- 13 government, the Department for Local Government if the agency is
- 14 a unit of government listed under KRS 61.931(1)(b) or (c) that is
- 15 not an organizational unit of the executive branch of state
- 16 government, the Kentucky Department of Education if the agency
- 17 is a public school district listed under KRS 61.931(1)(d), or the
- 18 Council on Postsecondary Education if the agency is an
- 19 educational entity listed under KRS 61.931(1)(e); and notify all
- 20 consumer credit reporting agencies included on the list maintained
- 21 by the Office of the Attorney General that compile and maintain
- 22 files on consumers on a nationwide basis, as defined in 15 U.S.C.
- 23 sec. 1681a(p), of the timing, distribution, and content of the notice;
- 24 or
- 25 2. If the agency determines that the misuse of **personally**
- 26 **identifiable**~~[personal]~~ information has not occurred and is not likely to
- 27 occur, the agency is not required to give notice, but shall maintain



1 records that reflect the basis for its decision for a retention period set by  
2 the State Archives and Records Commission as established by KRS  
3 171.420. The agency shall notify the appropriate entities listed in  
4 paragraph (a)1. of this subsection that the misuse of **personally**  
5 **identifiable**~~[personal]~~ information has not occurred.

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

- 9 1. Conspicuous posting of the notice on the Web site of the agency;
- 10 2. Notification to regional or local media if the security breach is localized,  
11 and also to major statewide media if the security breach is widespread,  
12 including broadcast media, such as radio and television; and
- 13 3. Personal communication to individuals whose data has been breached  
14 using the method listed in subdivision a., b., or c. of this subparagraph  
15 that the agency believes is most likely to result in actual notification to  
16 those individuals, if the agency has the information available:
  - 17 a. In writing, sent to the most recent address for the individual as  
18 reflected in the records of the agency;
  - 19 b. By **e-mail**~~[electronic mail]~~, sent to the most recent **e-**  
20 **mail**~~[electronic mail]~~ address for the individual as reflected in the  
21 records of the agency, unless the individual has communicated to  
22 the agency in writing that **he or she does**~~[they do]~~ not want **e-**  
23 **mail**~~[email]~~ notification **or the security breach involved**  
24 **information that the agency or nonaffiliated third party**  
25 **reasonably believes would permit an unauthorized person access**  
26 **to the e-mail account**; or
  - 27 c. By telephone, to the most recent telephone number for the

1 individual as reflected in the records of the agency.

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

3 1. To the extent possible, a description of the categories of information that  
4 were subject to the security breach, including the elements of personally  
5 identifiable~~[personal]~~ information that were or were believed to be  
6 acquired;

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

10 3. A description of the general acts of the agency, excluding disclosure of  
11 defenses used for the protection of information, to protect the personally  
12 identifiable~~[personal]~~ information from further security breach; and

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

16 a. The major consumer credit reporting agencies;

17 b. The Federal Trade Commission; and

18 c. The Office of the Kentucky Attorney General.

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

24 (3) (a) The notices required by subsection (1) of this section shall not be made if,  
25 after consultation with a law enforcement agency, the agency receives a  
26 written request from a law enforcement agency for a delay in notification  
27 because the notice may impede a criminal investigation. The written request

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

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

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

16 (5) This section shall not apply to:

17 (a) **Personally identifiable**~~personal~~ information:

18 **1.** That has been redacted;

19 **2.**~~(b)~~ ~~Personal information~~ Disclosed to a federal, state, or local  
 20 government entity, including a law enforcement agency or court, or their  
 21 agents, assigns, employees, or subcontractors, to investigate or conduct  
 22 criminal investigations and arrests or delinquent tax assessments, or to  
 23 perform any other statutory duties and responsibilities;

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

27 **4.**~~(d)~~ ~~Personal information~~ That an individual has consented to have

1 publicly disseminated or listed; or

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

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

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

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

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

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

19 (1) The department shall establish:

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

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

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

1 microphotographic process; and

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

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

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

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

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

17 As used in KRS 42.720 to 42.742:

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

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

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

- 1 (4) "Information technology" means data processing and telecommunications hardware,  
2 software, services, supplies, facilities, maintenance, and training that are used to  
3 support information processing and telecommunications systems to include  
4 geographic information systems;
- 5 (5) "**Personally identifiable**~~[personal]~~ information " has the same meaning as in KRS  
6 61.931;
- 7 (6) "Project" means a program to provide information technologies support to functions  
8 within an executive branch state agency, which should be characterized by well-  
9 defined parameters, specific objectives, common benefits, planned activities,  
10 expected outcomes and completion dates, and an established budget with a specified  
11 source of funding;
- 12 (7) "Security breach" has the same meaning as in KRS 61.931; and
- 13 (8) "Technology infrastructure" means any computing equipment, servers, networks,  
14 storage, desktop support, telephony, enterprise shared systems, information  
15 technology security, disaster recovery, business continuity, database administration,  
16 and software licensing.
- 17 ➔Section 12. KRS 42.726 is amended to read as follows:
- 18 (1) The roles and duties of the Commonwealth Office of Technology shall include but  
19 not be limited to:
- 20 (a) Providing technical support and services to all executive agencies of state  
21 government in the application of information technology;
- 22 (b) Assuring compatibility and connectivity of Kentucky's information systems;
- 23 (c) Developing strategies and policies to support and promote the effective  
24 applications of information technology within state government as a means of  
25 saving money, increasing employee productivity, and improving state services  
26 to the public, including electronic public access to information of the  
27 Commonwealth;

- 1 (d) Developing, implementing, and managing strategic information technology  
2 directions, standards, and enterprise architecture, including implementing  
3 necessary management processes to assure full compliance with those  
4 directions, standards, and architecture;
- 5 (e) Promoting effective and efficient design and operation of all major  
6 information resources management processes for executive branch agencies,  
7 including improvements to work processes;
- 8 (f) Developing, implementing, and maintaining the technology infrastructure of  
9 the Commonwealth and all related support staff, planning, administration,  
10 asset management, and procurement for all executive branch cabinets and  
11 agencies except:
- 12 1. Agencies led by a statewide elected official;
  - 13 2. The nine (9) public institutions of postsecondary education;
  - 14 3. The Department of Education's services provided to local school  
15 districts;
  - 16 4. The Kentucky Retirement Systems and the Teachers' Retirement  
17 System;
  - 18 5. The Kentucky Housing Corporation;
  - 19 6. The Kentucky Lottery Corporation;
  - 20 7. The Kentucky Higher Education Student Loan Corporation; and
  - 21 8. The Kentucky Higher Education Assistance Authority;
- 22 (g) Facilitating and fostering applied research in emerging technologies that offer  
23 the Commonwealth innovative business solutions;
- 24 (h) Reviewing and overseeing large or complex information technology projects  
25 and systems for compliance with statewide strategies, policies, and standards,  
26 including alignment with the Commonwealth's business goals, investment,  
27 and other risk management policies. The executive director is authorized to

- 1 grant or withhold approval to initiate these projects;
- 2 (i) Integrating information technology resources to provide effective and  
3 supportable information technology applications in the Commonwealth;
- 4 (j) Establishing a central statewide geographic information clearinghouse to  
5 maintain map inventories, information on current and planned geographic  
6 information systems applications, information on grants available for the  
7 acquisition or enhancement of geographic information resources, and a  
8 directory of geographic information resources available within the state or  
9 from the federal government;
- 10 (k) Coordinating multiagency information technology projects, including  
11 overseeing the development and maintenance of statewide base maps and  
12 geographic information systems;
- 13 (l) Providing access to both consulting and technical assistance, and education  
14 and training, on the application and use of information technologies to state  
15 and local agencies;
- 16 (m) In cooperation with other agencies, evaluating, participating in pilot studies,  
17 and making recommendations on information technology hardware and  
18 software;
- 19 (n) Providing staff support and technical assistance to the Geographic Information  
20 Advisory Council and the Kentucky Information Technology Advisory  
21 Council;
- 22 (o) Overseeing the development of a statewide geographic information plan with  
23 input from the Geographic Information Advisory Council;
- 24 (p) Developing for state executive branch agencies a coordinated security  
25 framework and model governance structure relating to the privacy and  
26 confidentiality of ***personally identifiable***~~[personal]~~ information collected and  
27 stored by state executive branch agencies, including but not limited to:



- 1           1. Identification of key infrastructure components and how to secure them;
- 2           2. Establishment of a common benchmark that measures the effectiveness
- 3           of security, including continuous monitoring and automation of
- 4           defenses;
- 5           3. Implementation of vulnerability scanning and other security
- 6           assessments;
- 7           4. Provision of training, orientation programs, and other communications
- 8           that increase awareness of the importance of security among agency
- 9           employees responsible for personally identifiable~~[personal]~~
- 10          information; and
- 11          5. Development of and making available a cyber security incident response
- 12          plan and procedure; and
- 13          (q) Preparing proposed legislation and funding proposals for the General
- 14          Assembly that will further solidify coordination and expedite implementation
- 15          of information technology systems.
- 16          (2) The Commonwealth Office of Technology may:
  - 17               (a) Provide general consulting services, technical training, and support for generic
  - 18               software applications, upon request from a local government, if the executive
  - 19               director finds that the requested services can be rendered within the
  - 20               established terms of the federally approved cost allocation plan;
  - 21               (b) Promulgate administrative regulations in accordance with KRS Chapter 13A
  - 22               necessary for the implementation of KRS 42.720 to 42.742, 45.253, 171.420,
  - 23               186A.040, 186A.285, and 194A.146;
  - 24               (c) Solicit, receive, and consider proposals from any state agency, federal agency,
  - 25               local government, university, nonprofit organization, private person, or
  - 26               corporation;
  - 27               (d) Solicit and accept money by grant, gift, donation, bequest, legislative

- 1 appropriation, or other conveyance to be held, used, and applied in accordance  
2 with KRS 42.720 to 42.742, 45.253, 171.420, 186A.040, 186A.285, and  
3 194A.146;
- 4 (e) Make and enter into memoranda of agreement and contracts necessary or  
5 incidental to the performance of duties and execution of its powers, including,  
6 but not limited to, agreements or contracts with the United States, other state  
7 agencies, and any governmental subdivision of the Commonwealth;
- 8 (f) Accept grants from the United States government and its agencies and  
9 instrumentalities, and from any source, other than any person, firm, or  
10 corporation, or any director, officer, or agent thereof that manufactures or sells  
11 information resources technology equipment, goods, or services. To these  
12 ends, the Commonwealth Office of Technology shall have the power to  
13 comply with those conditions and execute those agreements that are  
14 necessary, convenient, or desirable; and
- 15 (g) Purchase interest in contractual services, rentals of all types, supplies,  
16 materials, equipment, and other services to be used in the research and  
17 development of beneficial applications of information resources technologies.  
18 Competitive bids may not be required for:
- 19 1. New and emerging technologies as approved by the executive director or  
20 her or his designee; or
  - 21 2. Related professional, technical, or scientific services, but contracts shall  
22 be submitted in accordance with KRS 45A.690 to 45A.725.
- 23 (3) Nothing in this section shall be construed to alter or diminish the provisions of KRS  
24 171.410 to 171.740 or the authority conveyed by these statutes to the Archives and  
25 Records Commission and the Department for Libraries and Archives.
- 26 (4) The Commonwealth Office of Technology shall, on or before October 1 of each  
27 year, submit to the Legislative Research Commission a report in accordance with

- 1           KRS 57.390 detailing:
- 2           (a) Any security breaches that occurred within organizational units of the
- 3                 executive branch of state government during the prior fiscal year that required
- 4                 notification to the Commonwealth Office of Technology under KRS 61.932;
- 5           (b) Actions taken to resolve the security breach, and to prevent additional security
- 6                 breaches in the future;
- 7           (c) A general description of what actions are taken as a matter of course to protect
- 8                 personal data from security breaches; and
- 9           (d) Any quantifiable financial impact to the agency reporting a security breach.

10           ➔Section 13. Whereas consumer reporting agencies maintain sensitive identifying

11 information of millions of consumers and play a critical role in the consumer financial

12 services marketplace, and the prevalence of security breaches containing sensitive

13 identifying information of consumers is on the rise, as is the accompanying risk of

14 identity theft for those consumers exposed as a result of these breaches, an emergency is

15 declared to exist, and this Act takes effect upon its passage and approval by the Governor

16 or upon its otherwise becoming a law.