

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**  
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) 1. Providing the consumer, at no charge, at least one (1) copy of his or**  
21 **her consumer report each year from each nationwide consumer**  
22 **reporting agency. This copy shall be in addition to the free annual**  
23 **disclosure under 15 U.S.C. sec. 1681j to which the consumer may be**  
24 **entitled.**

25 **2. If the requirement for a free annual disclosure under 15 U.S.C. sec.**  
26 **1681j is repealed or otherwise becomes no longer applicable, the**  
27 **number of copies of a consumer report required to be provided under**

- 1                   subparagraph 1. of this paragraph shall be at least two (2) consumer  
2                   reports each year from each nationwide consumer reporting agency;
- 3                   (b) Daily monitoring of a consumer's consumer report at each nationwide  
4                   consumer reporting agency; and
- 5                   (c) Alerting a consumer by telephone, e-mail, or text when there are changes in  
6                   his or her consumer report at any nationwide consumer reporting agency;
- 7                   (6) "Encrypt" has the same meaning as in Section 5 of this Act;
- 8                   (7) "Nationwide consumer reporting agency" means a consumer reporting agency  
9                   that compiles and maintains files on consumers on a nationwide basis as defined  
10                   by the Fair Credit Reporting Act, 15 U.S.C. sec. 1681a(p);
- 11                   (8) "Personally identifiable information" means a consumer's first name or first  
12                   initial and last name, personal mark, or unique biometric or genetic print or  
13                   image, in combination with any one (1) or more of the following data elements:
- 14                   (a) A financial account number, credit card number, or debit card number,  
15                   with or without any security code, security question and answer, access  
16                   code, or password that permits access to a consumer's account;
- 17                   (b) A user name or e-mail address with any security code, security question and  
18                   answer, access code, or password that permits access to any account of the  
19                   consumer that stores financial data;
- 20                   (c) A Social Security number;
- 21                   (d) A tax identification number that incorporates a Social Security number;
- 22                   (e) A driver's license number, state identification card number, or other  
23                   identification number issued by a state;
- 24                   (f) A passport number or other identification number issued by the United  
25                   States government; or
- 26                   (g) Individually identifiable health information as defined in 45 C.F.R. sec.  
27                   160.103;

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

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

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

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

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

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

17 (10)[(4)] "Security freeze" means a notice placed on a consumer file, at the request of  
 18 the consumer and subject to certain exceptions, that prohibits a consumer reporting  
 19 agency from releasing the consumer's consumer report or credit score relating to the  
 20 extension of credit without the express authorization of the consumer; and

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

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

25 (1) For the purposes of this section:

26 (a) "Protected person" means an individual who is under sixteen (16) years of age  
 27 at the time a request for the placement of a security freeze is made, or who is

1 an incapacitated person or other person for whom a guardian or conservator  
2 has been appointed;

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

- 4 1. Identifies a protected person;
- 5 2. Is created by a consumer reporting agency solely for the purpose of  
6 complying with this section; and
- 7 3. Is not created or used to consider the protected person's  
8 creditworthiness, credit standing, credit capacity, character, general  
9 reputation, personal characteristics, or mode of living;

10 (c) "Representative" means a person who provides to a consumer reporting  
11 agency sufficient proof of authority to act on behalf of a protected person; and

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

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

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

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

25 (b) The protected person's representative:

- 26 1. Submits the request to the consumer reporting agency using the method  
27 that the agency has established to receive security freeze requests~~at~~

- 1                   ~~the address designated by the consumer reporting agency to receive the~~  
2                   ~~request~~];
- 3                   2. Provides to the consumer reporting agency clear and proper  
4                   identification of the protected person and the representative;
- 5                   3. Provides to the consumer reporting agency sufficient proof of authority  
6                   to act on behalf of the protected person; and
- 7                   4. Pays to the consumer reporting agency a fee as prescribed in subsection  
8                   (8) of this section.
- 9 (3) If a consumer reporting agency does not have a file pertaining to a protected person  
10 when the consumer reporting agency receives a request pursuant to subsection (2) of  
11 this section, the consumer reporting agency shall create a record for the protected  
12 person.
- 13 (4) Within thirty (30) days after receiving a request pursuant to this section, a consumer  
14 reporting agency shall place a security freeze on the protected person's record or  
15 consumer~~[credit]~~ report.
- 16 (5) Unless a security freeze is removed pursuant to subsection (7) or (10) of this  
17 section, a consumer reporting agency may not release the protected person's  
18 consumer~~[credit]~~ report, any information derived from the protected person's  
19 consumer~~[credit]~~ report, or any record created for the protected person.
- 20 (6) A security freeze that is placed on a protected person's record or consumer~~[credit]~~  
21 report placed under this section remains in effect until either:
- 22 (a) The protected person or the protected person's representative requests that the  
23 consumer reporting agency remove the security freeze pursuant to subsection  
24 (7) of this section; or
- 25 (b) The security freeze is removed pursuant to subsection (10) of this section.
- 26 (7) (a) To remove a security freeze for a protected person, the protected person or the  
27 protected person's representative shall submit a request for the removal of the

1 security freeze to the consumer reporting agency at the address designated by  
2 the consumer reporting agency to receive the request, and pay a fee as  
3 prescribed in subsection (8) of this section. In addition:

4 1. If the protected person requested the removal of the security freeze, the  
5 protected person shall provide to the consumer reporting agency  
6 ~~both~~~~either~~ of the following:

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

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

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

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

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

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

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

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

27 (a) The protected person or the protected person's representative has received a

1           notification of a security breach pursuant to Section 3, 4, or 7 of this Act  
 2           that affects the protected person and, upon request, provides a copy of the  
 3           notification to the consumer reporting agency;

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

8           **(c)**~~(b)~~ A request for the placement or removal of a security freeze is for a  
 9           protected person who is under sixteen (16) years of age at the time of the  
 10           request and the consumer reporting agency has a **consumer**~~credit~~ report  
 11           pertaining to the protected person.

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

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

19           (a) Any actual damages sustained by the **protected person**~~consumer~~ as a result  
 20           of the failure;

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

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

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

27       (12) Any person, other than the named individual or individuals in the report, who

1 obtains a consumer report, requests a security freeze~~], requests the temporary lift of~~  
2 ~~a freeze]~~, or requests the removal of a security freeze from a consumer reporting  
3 agency under false pretenses or in an attempt to violate federal or state law shall be  
4 liable to the consumer reporting agency for actual damages sustained by the  
5 consumer reporting agency or one thousand dollars (\$1,000), whichever is greater.

6 (13) This section does not apply to a protected person's consumer~~[credit]~~ report or  
7 record provided to:

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

- 1 (f) A child support enforcement agency;
- 2 (g) A consumer reporting agency that acts only as a reseller of credit information  
3 by assembling and merging information contained in the database of another  
4 consumer reporting agency or multiple credit reporting agencies and does not  
5 maintain a permanent database of credit information from which new  
6 consumer reports are produced. However, a consumer reporting agency acting  
7 as a reseller shall honor any security freeze placed on a consumer report by  
8 another consumer reporting agency;
- 9 (h) A check services or fraud prevention services company that~~[, which]~~ issues  
10 reports on incidents of fraud or authorizations for the purpose of approving or  
11 processing negotiable instruments, electronic funds transfers, or similar  
12 methods of payments;
- 13 (i) A deposit account information service company that~~[, which]~~ issues reports  
14 regarding account closures due to fraud, substantial overdrafts, ATM abuse, or  
15 similar negative information regarding a consumer to inquiring banks or other  
16 financial institutions for use only in reviewing a consumer request for a  
17 deposit account at the inquiring bank or financial institution;
- 18 (j) Any person or entity using a consumer report in preparation for a civil or  
19 criminal action, or an insurance company in investigation of a claim; or
- 20 (k) 1. Any insurance company for setting or adjusting a rate or underwriting  
21 for property and casualty insurance purposes; or  
22 2. Any consumer reporting agency database or file which consists solely of  
23 consumer information concerning, and used solely for:  
24 a. Criminal record information;  
25 b. Personal loss history information;  
26 c. Fraud prevention or detection;  
27 d. Employment screening; or

1 e. Tenant screening.

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

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

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

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

6 **1. In the possession or control of the consumer reporting agency or a**  
 7 **third-party agent; and**

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

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

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

27 ~~(3)(2)~~ The consumer reporting agency shall, no later than ten (10) business days after

1 the date the agency receives the request for a security freeze, provide the consumer  
2 with a unique personal identification number or password to be used by the  
3 consumer when providing authorization for the access to his or her credit file for a  
4 specific period of time. In addition, the consumer reporting agency shall  
5 simultaneously provide to the consumer in writing the process of placing, removing,  
6 and temporarily lifting a security freeze and the process for allowing access to  
7 information from the consumer's credit file for a specific period while the security  
8 freeze is in effect.

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

21 ~~(5)~~~~(4)~~ If a third party requests access to a consumer report on which a security freeze  
22 is in effect, and this request is in connection with an application for credit, the third  
23 party may treat the application as incomplete.

24 ~~(6)~~~~(5)~~ If the consumer wishes to allow his **or her** consumer report or credit score to  
25 be accessed for a specific period of time while a freeze is in place, the consumer  
26 shall contact the consumer reporting agency and request that the freeze be  
27 temporarily lifted and provide the following:

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

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

15 ~~(8) [(7)]~~ A consumer reporting agency shall remove or temporarily lift a freeze placed  
16 on a consumer's consumer report only~~[ in the following cases ]~~:

- 17 (a) Upon **the consumer's**~~[consumer]~~ request **made pursuant to subsection (6) or**  
18 **(9) of**~~[as provided in]~~ this section; or
- 19 (b) If the~~[consumer's]~~ consumer report was frozen due to a material  
20 misrepresentation of fact by the consumer. If a consumer reporting agency  
21 intends to remove a freeze upon a~~[consumer's]~~ consumer report pursuant to  
22 this paragraph, the consumer reporting agency shall notify the consumer in  
23 writing prior to removing the freeze on the~~[consumer's]~~ consumer report.

24 ~~(9) [(8)]~~ A security freeze shall remain in place until the consumer requests that the  
25 security freeze be removed, **or the consumer reporting agency has notified the**  
26 **consumer in writing that it is removing the freeze due to a misrepresentation of**  
27 **fact by the consumer pursuant to subsection (8)(b) of this section**~~[but no longer~~

1 ~~than seven (7) years from the date the security freeze was put in place~~. A consumer  
2 reporting agency shall remove a security freeze within three (3) business days of  
3 receiving;

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

5 (b) Both of the following:

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

7 ~~2. (b)~~ The unique personal identification number or password provided  
8 by the consumer reporting agency.

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

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

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

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

26 (d) A subsidiary, affiliate, agent, assignee, or prospective assignee of a person to  
27 whom access has been granted under subsection (6)~~(5)~~ of this section for the

- 1 purposes of facilitating the extension of credit;
- 2 (e) A person~~[,]~~ for the purposes of prescreening as provided by the~~[federal]~~ Fair  
3 Credit Reporting Act, 15 U.S.C. secs. 1681 et seq.;
- 4 (f) A consumer reporting agency for the purposes of providing a consumer with a  
5 copy of his or her own report on the consumer's~~[his]~~ request;
- 6 (g) A child support enforcement agency;
- 7 (h) A consumer reporting agency that acts only as a reseller of credit information  
8 by assembling and merging information contained in the database of another  
9 consumer reporting agency or multiple credit reporting agencies and does not  
10 maintain a permanent database of credit information from which new  
11 consumer reports are produced. However, a consumer reporting agency acting  
12 as a reseller shall honor any security freeze placed on a consumer report by  
13 another consumer reporting agency;
- 14 (i) A check services or fraud prevention services company that~~[, which]~~ issues  
15 reports on incidents of fraud or authorizations for the purpose of approving or  
16 processing negotiable instruments, electronic funds transfers, or similar  
17 methods of payments;
- 18 (j) A deposit account information service company that~~[, which]~~ issues reports  
19 regarding account closures due to fraud, substantial overdrafts, ATM abuse, or  
20 similar negative information regarding a consumer to inquiring banks or other  
21 financial institutions for use only in reviewing a consumer request for a  
22 deposit account at the inquiring bank or financial institution;
- 23 (k) Any person or entity using a consumer report in preparation for a civil or  
24 criminal action, or an insurance company in investigation of a claim; or
- 25 (l) Any insurance company for setting or adjusting a rate or underwriting for  
26 property and casualty insurance purposes.
- 27 (11)~~(10)~~ A consumer reporting agency may impose a reasonable charge on a consumer

1 for initially placing, temporarily lifting, or removing a security freeze on a consumer  
 2 file. The amount of the charge may not exceed ten dollars (\$10). On January 1 of  
 3 each year, a consumer reporting agency may increase the charge for placing a  
 4 security ~~freeze~~~~alert~~. The increase shall be based proportionally on changes to the  
 5 Consumer Price Index for All Urban Consumers as determined by the United States  
 6 Department of Labor with fractional changes rounded to the nearest twenty-five  
 7 cents (\$0.25).~~An exception shall be allowed whereby the consumer will be~~  
 8 ~~charged zero dollars by the consumer reporting agency placing the security freeze~~  
 9 ~~if~~

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

12 **(a)** The consumer:

13 **1. Has received a notification of a security breach pursuant to subsection**  
 14 **(14) of this section, or Section 4 or 7 of this Act that affects the**  
 15 **consumer; or**

16 **2.** Is a victim of identity theft; and~~;~~

17 **(b)** Upon ~~the~~ request ~~of the consumer reporting agency~~, **the consumer**  
 18 provides the consumer reporting agency with a **copy of a** valid police report **or**  
 19 **the notification of the security breach.**

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

24 **1.**~~(a)~~ Name;

25 **2.**~~(b)~~ Date of birth;

26 **3.**~~(c)~~ Social Security number; and

27 **4.**~~(d)~~ Address.

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

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

8       **(a) As soon as possible and without unreasonable delay, but no later than**  
9       **thirty-five (35) days following discovery of a security breach, notify the**  
10       **consumer of the security breach in compliance with the requirements of**  
11       **subsections (4) to (7) of Section 4 of this Act; and**

12       **(b) For a period of three (3) years following the breach:**

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

15               **2. Reimburse the consumer for credit monitoring purchased by the**  
16               **consumer.**

17       **(15) An individual, including but not limited to a protected person or his or her**  
18       **representative as defined in Section 2 of this Act, who requests the placement of,**  
19       **a temporary lift of, or removal of a security freeze with a nationwide consumer**  
20       **reporting agency shall have the option to have the request sent to any other**  
21       **nationwide consumer reporting agency and applied to the corresponding**  
22       **consumer report for that agency if the individual:**

23       **(a) Has been notified of a security breach pursuant to subsection (14) of this**  
24       **section, or Section 4 or 7 of this Act; or**

25       **(b) Is a victim of identity theft.**

26       **(16) A third-party agent shall notify the consumer reporting agency of any security**  
27       **breach relating to the consumer reporting agency's records or data as soon as**

1        reasonably practicable, but not later than seventy-two (72) hours, following  
2        discovery.

3        (17) A consumer reporting agency shall comply with subsections (3) and (9) of Section  
4        4 of this Act.

5        (18)~~(12)~~ Any person who willfully fails to comply with any requirement imposed under  
6        this section with respect to any consumer is liable to that consumer in an amount  
7        equal to the sum of:

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

15       (19)~~(13)~~ Any person, other than the named individual or individuals in the report, who  
16       obtains a consumer report, requests a security freeze, requests the temporary lift of a  
17       freeze, or the removal of a security freeze from a consumer reporting agency under  
18       false pretenses or in an attempt to violate federal or state law shall be liable to the  
19       consumer reporting agency for actual damages sustained by the consumer reporting  
20       agency or one thousand dollars (\$1,000), whichever is greater.

21       (20)~~(14)~~ Any person who is negligent in failing to comply with any requirement  
22       imposed under this section with respect to any consumer is liable to that consumer  
23       in an amount equal to the sum of:

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

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

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

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

5 **(22)**~~(15)~~ Nothing in KRS 367.363 to 367.365 shall be construed to limit or restrict the  
 6 exercise of powers or the performance of the duties of the Attorney General  
 7 authorized under any other provision of law to bring or seek redress for persons that  
 8 violate KRS 367.363 to 367.365.

9 ➔Section 4. KRS 365.732 is amended to read as follows:

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

11 (a) **"Encrypt" has the same meaning as in Section 5 of this Act**~~["Breach of the~~  
 12 ~~security of the system" means unauthorized acquisition of unencrypted and~~  
 13 ~~unredacted computerized data that compromises the security, confidentiality,~~  
 14 ~~or integrity of personally identifiable information maintained by the~~  
 15 ~~information holder as part of a database regarding multiple individuals that~~  
 16 ~~actually causes, or leads the information holder to reasonably believe has~~  
 17 ~~caused or will cause, identity theft or fraud against any resident of the~~  
 18 ~~Commonwealth of Kentucky. Good faith acquisition of personally identifiable~~  
 19 ~~information by an employee or agent of the information holder for the~~  
 20 ~~purposes of the information holder is not a breach of the security of the system~~  
 21 ~~if the personally identifiable information is not used or subject to further~~  
 22 ~~unauthorized disclosure];~~

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

25 (c) **"Personally identifiable information" means a consumer's first name or**  
 26 **first initial and last name, personal mark, or unique biometric or genetic**  
 27 **print or image, in combination with any one (1) or more of the following**

1 data elements:

2 1. A financial account number, credit card number, or debit card  
3 number, with or without any security code, security question and  
4 answer, access code, or password that permits access to a consumer's  
5 account;

6 2. A user name or e-mail address with any security code, security  
7 question and answer, access code, or password that permits access to  
8 any account of the consumer that stores financial data;

9 3. A Social Security number;

10 4. A tax identification number that incorporates a Social Security  
11 number;

12 5. A driver's license number, state identification card number, or other  
13 identification number issued by a state;

14 6. A passport number or other identification number issued by the  
15 United States government; or

16 7. Individually identifiable health information as defined in 45 C.F.R.  
17 sec. 160.103; and

18 (d) 1. "Security breach" means the unauthorized acquisition, distribution,  
19 disclosure, destruction, or manipulation of, or access to, an  
20 information holder's records or data that:

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

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

25 2. "Security breach" does not include:

26 a. The good-faith acquisition of or access to personally identifiable  
27 information by an employee or agent of the information holder if

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

3 *b. The acquisition, distribution, or disclosure of, or access to,*  
 4 *encrypted or redacted records or data without the accompanying*  
 5 *acquisition of or reasonable ability to access or discover the*  
 6 *confidential process or key necessary to unencrypt or decipher*  
 7 *the records or data*["Personally identifiable information" means an  
 8 individual's first name or first initial and last name in combination  
 9 with any one (1) or more of the following data elements, when the  
 10 name or data element is not redacted:

- 11 1. Social Security number;
- 12 2. Driver's license number; or
- 13 3. Account number or credit or debit card number, in combination with any  
 14 required security code, access code, or password to permit access to an  
 15 individual's financial account].

16 (2) *For each resident of Kentucky affected by a security breach, the*[Any] information  
 17 holder *whose records or data have been breached* shall:

18 *(a) Notify the resident of the security breach as soon as*[disclose any breach of  
 19 the security of the system, following discovery or notification of the breach in  
 20 the security of the data, to any resident of Kentucky whose unencrypted  
 21 personal information was, or is reasonably believed to have been, acquired by  
 22 an unauthorized person. The disclosure shall be made in the most expedient  
 23 time] possible and without unreasonable delay, *but no later than thirty-five*  
 24 *(35) days following discovery of the breach,* consistent with the legitimate  
 25 needs of law enforcement, as provided in subsection (4) of this section, or any  
 26 measures necessary to determine the scope of the breach and restore the  
 27 reasonable integrity of the *records or* data[system];

1 (b) Provide or offer the resident one (1) copy of his or her consumer report  
 2 from each nationwide consumer reporting agency at no cost to the resident.

3 The copies of a consumer report required under this paragraph shall be:

4 1. In addition to the free annual disclosure under 15 U.S.C. sec. 1681j to  
 5 which the consumer may be entitled; and

6 2. Requested by the resident within the twelve (12) month period  
 7 immediately following the receipt of the notice of a security breach.

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, **each nationwide**~~[all]~~ consumer reporting  
23 **agency**~~[agencies and credit bureaus that compile and maintain files on consumers~~  
24 ~~on a nationwide basis, as defined by 15 U.S.C. sec. 1681a,]~~ of the timing,  
25 distribution, and content of the notices.

26 (8) **An individual shall not, as a condition of exercising his or her rights under any**  
27 **provision of this section, be required to:**

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

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

3 (9) An information holder who owns or licenses the personally identifiable  
 4 information of more than one thousand (1,000) residents of the Commonwealth  
 5 of Kentucky shall encrypt all personally identifiable information electronically  
 6 transmitted or stored by that information holder. If the personally identifiable  
 7 information is not stored electronically, the information holder shall develop,  
 8 implement, and maintain alternative compensating controls consistent with  
 9 industry standards and the information holder's assessment of risk, to protect the  
 10 security, confidentiality, and integrity of the personally identifiable information.

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

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

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

17 2. The ~~federal~~ Health Insurance Portability and Accountability Act of  
 18 1996, Pub. L. No. 104-191, as amended;~~[,] or~~

19 (b) Any agency of the Commonwealth of Kentucky or any of its local  
 20 governments or political subdivisions; or

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

22 ➔Section 5. KRS 61.931 is amended to read as follows:

23 As used in KRS 61.931 to 61.934:

24 (1) "Agency" means:

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

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

- 1 government;
- 2 (c) Every organizational unit, department, division, branch, section, unit, office,  
3 administrative body, program cabinet, bureau, board, commission, committee,  
4 subcommittee, ad hoc committee, council, authority, public agency,  
5 instrumentality, interagency body, special purpose governmental entity, or  
6 public corporation of an entity specified in paragraph (a) or (b) of this  
7 subsection or created, established, or controlled by an entity specified in  
8 paragraph (a) or (b) of this subsection;
- 9 (d) Every public school district in the Commonwealth of Kentucky; and
- 10 (e) Every public institution of postsecondary education, including every public  
11 university in the Commonwealth of Kentucky and public college of the entire  
12 Kentucky Community and Technical College System;
- 13 (2) "Commonwealth Office of Technology" means the office established by KRS  
14 42.724;
- 15 (3) "Encrypt~~Encryption~~" means the conversion of data using technology that:  
16 (a) Meets or exceeds the level adopted by the National Institute of Standards  
17 Technology as part of the Federal Information Processing Standards;~~[-]~~ and  
18 (b) Renders the data indecipherable without the associated cryptographic key to  
19 decipher the data;
- 20 (4) "Law enforcement agency" means any lawfully organized investigative agency,  
21 sheriff's office, police unit, or police force of federal, state, county, urban-county  
22 government, charter county, city, consolidated local government, unified local  
23 government, or any combination of these entities, responsible for the detection of  
24 crime and the enforcement of the general criminal federal and state laws;
- 25 (5) (a) "Nonaffiliated third party" means any person that:  
26 1.~~[(a)]~~ Has a contract or agreement with an agency; and  
27 2.~~[(b)]~~ Receives personally identifiable~~personal~~ information from the

1 agency pursuant to the contract or agreement.

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

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

4 **a. Title V of the Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-**  
 5 **102, as amended; or**

6 **b. The Health Insurance Portability and Accountability Act of**  
 7 **1996, Pub. L. No. 104-191, as amended; or**

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

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

13 (a) **A financial**~~An~~ account number, credit card number, or debit card number,  
 14 ~~[that, in combination]~~with **or without** any ~~[required]~~security code, **security**  
 15 **question and answer,** access code, or password **that permits**~~;~~~~would permit]~~  
 16 access to **the individual's**~~an~~ account;

17 **(b) A user name or e-mail address with any security code, security question and**  
 18 **answer, access code, or password that permits access to any account of the**  
 19 **individual that stores financial data;**

20 **(c)**~~(b)~~ A Social Security number;

21 **(d)**~~(e)~~ A taxpayer identification number that incorporates a Social Security  
 22 number;

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

25 **(f)**~~(e)~~ A passport number or other identification number issued by the United  
 26 States government; or

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

1 160.103, except for education records covered by the Family Educational  
2 Rights and Privacy Act, as amended, 20 U.S.C. sec. 1232g;

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

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

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

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

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

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

22 ~~2. [The unauthorized acquisition, distribution, disclosure, destruction,~~  
23 ~~manipulation, or release of encrypted records or data containing personal~~  
24 ~~information along with the confidential process or key to unencrypt the~~  
25 ~~records or data that compromises or the agency or nonaffiliated third~~  
26 ~~party reasonably believes may compromise the security, confidentiality,~~  
27 ~~or integrity of personal information and ]Results[result] in the likelihood~~

1 of harm to one (1) or more individuals.

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

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

12 ➔Section 6. KRS 61.932 is amended to read as follows:

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

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

- 14 (c) 1. If an agency is subject to any additional requirements under the  
15 Kentucky Revised Statutes or under federal law, protocols, or  
16 agreements relating to the protection and privacy of **personally**  
17 **identifiable**~~personally~~ information, the agency shall comply with these  
18 additional requirements, in addition to the requirements of KRS 61.931  
19 to 61.934.
- 20 2. If a nonaffiliated third party is required by federal law or regulation to  
21 conduct security breach investigations or to make notifications of  
22 security breaches, or both, as a result of the nonaffiliated third party's  
23 unauthorized disclosure of one (1) or more data elements of **personally**  
24 **identifiable**~~personally~~ information that is the same as one (1) or more of  
25 the data elements of **personally identifiable**~~personally~~ information listed  
26 in KRS 61.931(6)(a) to ~~(g)~~~~(f)~~, the nonaffiliated third party shall meet  
27 the requirements of KRS 61.931 to 61.934 by providing to the agency a

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

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

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

1 subsection shall specify how the cost of the notification and  
2 investigation requirements under KRS 61.933 are to be apportioned  
3 when a security breach is suffered by the agency or nonaffiliated third  
4 party.

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

18 ➔Section 7. KRS 61.933 is amended to read as follows:

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

25 1. Notify the commissioner of the Kentucky State Police, the Auditor of  
26 Public Accounts, and the Attorney General. In addition, an agency shall  
27 notify the secretary of the Finance and Administration Cabinet or his or

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

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

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

- 20 1. If the agency determined that a security breach has occurred and that the  
21 misuse of personally identifiable~~personal~~ information has occurred or  
22 is reasonably likely to occur, the agency shall:
- 23 a. Within forty-eight (48) hours of completion of the investigation,  
24 notify in writing all officers listed in paragraph (a)1. of this  
25 subsection, and the commissioner of the Department for Libraries  
26 and Archives, unless the provisions of subsection (3) of this  
27 section apply;

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

1           171.420. The agency shall notify the appropriate entities listed in  
2           paragraph (a)1. of this subsection that the misuse of **personally**  
3           **identifiable**~~[personal]~~ information has not occurred.

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

7           1. Conspicuous posting of the notice on the Web site of the agency;  
8           2. Notification to regional or local media if the security breach is localized,  
9           and also to major statewide media if the security breach is widespread,  
10          including broadcast media, such as radio and television; and

11          3. Personal communication to individuals whose data has been breached  
12          using the method listed in subdivision a., b., or c. of this subparagraph  
13          that the agency believes is most likely to result in actual notification to  
14          those individuals, if the agency has the information available:

15          a. In writing, sent to the most recent address for the individual as  
16          reflected in the records of the agency;

17          b. By **e-mail**~~[electronic mail]~~, sent to the most recent **e-**  
18          **mail**~~[electronic mail]~~ address for the individual as reflected in the  
19          records of the agency, unless the individual has communicated to  
20          the agency in writing that **he or she does**~~[they do]~~ not want **e-**  
21          **mail**~~[email]~~ notification **or the security breach involved**  
22          **information that the agency or nonaffiliated third party**  
23          **reasonably believes would permit an unauthorized person access**  
24          **to the e-mail account**; or

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

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

- 1           1.    To the extent possible, a description of the categories of information that  
2                    were subject to the security breach, including the elements of personally  
3                    identifiable~~[personal]~~ information that were or were believed to be  
4                    acquired;
- 5           2.    Contact information for the notifying agency, including the address,  
6                    telephone number, and toll-free number if a toll-free number is  
7                    maintained;
- 8           3.    A description of the general acts of the agency, excluding disclosure of  
9                    defenses used for the protection of information, to protect the personally  
10                   identifiable~~[personal]~~ information from further security breach; and
- 11          4.    The toll-free numbers, addresses, and Web site addresses, along with a  
12                    statement that the individual can obtain information from the following  
13                    sources about steps the individual may take to avoid identity theft, for:
  - 14                    a.    The major consumer credit reporting agencies;
  - 15                    b.    The Federal Trade Commission; and
  - 16                    c.    The Office of the Kentucky Attorney General.
- 17          (c)    The agency providing notice pursuant to this subsection shall cooperate with  
18                    any investigation conducted by the agencies notified under subsection (1)(a)  
19                    of this section and with reasonable requests from the Office of Consumer  
20                    Protection of the Office of the Attorney General, consumer credit reporting  
21                    agencies, and recipients of the notice, to verify the authenticity of the notice.
- 22          (3)   (a)    The notices required by subsection (1) of this section shall not be made if,  
23                    after consultation with a law enforcement agency, the agency receives a  
24                    written request from a law enforcement agency for a delay in notification  
25                    because the notice may impede a criminal investigation. The written request  
26                    may apply to some or all of the required notifications, as specified in the  
27                    written request from the law enforcement agency. Upon written notification

1 from the law enforcement agency that the criminal investigation has been  
 2 completed, or that the sending of the required notifications will no longer  
 3 impede a criminal investigation, the agency shall send the notices required by  
 4 subsection (1)(b)1. of this section.

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

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

14 (5) This section shall not apply to:

15 (a) **Personally identifiable**~~[personal]~~ information;

16 **1.** ~~[That has been redacted;~~

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

22 **2.**~~[(e)]~~ ~~[Personal information —]~~ That is publicly and lawfully made  
 23 available to the general public from federal, state, or local government  
 24 records; **or**

25 **3.**~~[(d)]~~ ~~[Personal information —]~~ That an individual has consented to have  
 26 publicly disseminated or listed; or

27 **(b)**~~[(e)]~~ Any document recorded in the records of either a county clerk or circuit

1 clerk of a county, or in the records of a United States District Court.

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

7 ➔Section 8. KRS 61.934 is amended to read as follows:

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

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

16 ➔Section 9. KRS 171.450 is amended to read as follows:

17 (1) The department shall establish:

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

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

24 (c) Standards and procedures for recording, managing, and preserving public  
25 records and for the reproduction of public records by photographic or  
26 microphotographic process; and

27 (d) Procedures for collection and distribution by the central depository of all

1 reports and publications, except the Kentucky Revised Statutes editions,  
2 issued by any department, board, commission, officer or other agency of the  
3 Commonwealth for general public distribution after July 1, 1958.

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

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

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

14 ➔Section 10. KRS 42.722 is amended to read as follows:

15 As used in KRS 42.720 to 42.742:

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

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

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

26 (4) "Information technology" means data processing and telecommunications hardware,  
27 software, services, supplies, facilities, maintenance, and training that are used to

1 support information processing and telecommunications systems to include  
2 geographic information systems;

3 (5) "***Personally identifiable***~~[personal]~~ information " has the same meaning as in KRS  
4 61.931;

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

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

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

15 ➔Section 11. KRS 42.726 is amended to read as follows:

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

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

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

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

26 (d) Developing, implementing, and managing strategic information technology  
27 directions, standards, and enterprise architecture, including implementing

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

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

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

1 194A.146;

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

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

13 (g) Purchase interest in contractual services, rentals of all types, supplies,  
14 materials, equipment, and other services to be used in the research and  
15 development of beneficial applications of information resources technologies.

16 Competitive bids may not be required for:

- 17 1. New and emerging technologies as approved by the executive director or  
18 her or his designee; or  
19 2. Related professional, technical, or scientific services, but contracts shall  
20 be submitted in accordance with KRS 45A.690 to 45A.725.

21 (3) Nothing in this section shall be construed to alter or diminish the provisions of KRS  
22 171.410 to 171.740 or the authority conveyed by these statutes to the Archives and  
23 Records Commission and the Department for Libraries and Archives.

24 (4) The Commonwealth Office of Technology shall, on or before October 1 of each  
25 year, submit to the Legislative Research Commission a report in accordance with  
26 KRS 57.390 detailing:

27 (a) Any security breaches that occurred within organizational units of the

1 executive branch of state government during the prior fiscal year that required  
2 notification to the Commonwealth Office of Technology under KRS 61.932;

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

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

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

8 ➔Section 12. Whereas consumer reporting agencies maintain sensitive identifying  
9 information of millions of consumers and play a critical role in the consumer financial  
10 services marketplace, and the prevalence of security breaches containing sensitive  
11 identifying information of consumers is on the rise, as is the accompanying risk of  
12 identity theft for those consumers exposed as a result of these breaches, an emergency is  
13 declared to exist, and this Act takes effect upon its passage and approval by the Governor  
14 or upon its otherwise becoming a law.