61.933 Notification of personal information security breach -- Investigation -- Notice to affected individuals of result of investigation -- Personal information not subject to requirements -- Injunctive relief by Attorney General.

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

1. Notify the commissioner of the Kentucky State Police, the Auditor of Public Accounts, and the Attorney General. In addition, an agency shall notify the secretary of the Finance and Administration Cabinet or his or her designee if an agency is an organizational unit of the executive branch of state government; notify the commissioner of the Department for Local Government if the agency is a unit of government listed in KRS 61.931(1)(b) or (c) that is not an organizational unit of the executive branch of state government; notify the commissioner of the Kentucky Department of Education if the agency is a public school district listed in KRS 61.931(1)(d); and notify the president of the Council on Postsecondary Education if the agency is an educational entity listed under KRS 61.931(1)(e). Notification shall be in writing on a form developed by the Commonwealth Office of Technology. The Commonwealth Office of Technology shall promulgate administrative regulations KRS 61.931 to 61.934 regarding the contents of the form; and
2. Begin conducting a reasonable and prompt investigation in accordance with the security and breach investigation procedures and practices referenced in KRS 61.932(1)(b) to determine whether the security breach has resulted in or is likely to result in the misuse of the personal information.

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

1. If the agency determined that a security breach has occurred and that the misuse of personal information has occurred or is reasonably likely to occur, the agency shall:
   a. Within forty-eight (48) hours of completion of the investigation, notify in writing all officers listed in paragraph (a)1. of this subsection, and the commissioner of the Department for Libraries and Archives, unless the provisions of subsection (3) of this section apply;
   b. Within thirty-five (35) days of providing the notifications required by subdivision a. of this subparagraph, notify all individuals impacted by the security breach as provided in subsection (2) of this section, unless the provisions of subsection (3) of this section apply; and
   c. If the number of individuals to be notified exceeds one thousand (1,000), the agency shall notify, at least seven (7)

days prior to providing notice to individuals under subdivision b. of this subparagraph, the Commonwealth Office of Technology if the agency is an organizational unit of the executive branch of state government, the Department for Local Government if the agency is a unit of government listed under KRS 61.931(1)(b) or (c) that is not an organizational unit of the executive branch of state government, the Kentucky Department of Education if the agency is a public school district listed under KRS 61.931(1)(d), or the Council on Postsecondary Education if the agency is an educational entity listed under KRS 61.931(1)(e); and notify all consumer credit reporting agencies included on the list maintained by the Office of the Attorney General that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. sec. 1681a(p), of the timing, distribution, and content of the notice; or

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

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

1. Conspicuous posting of the notice on the Web site of the agency;
2. Notification to regional or local media if the security breach is localized, and also to major statewide media if the security breach is widespread, including broadcast media, such as radio and television; and
3. Personal communication to individuals whose data has been breached using the method listed in subdivision a., b., or c. of this subparagraph that the agency believes is most likely to result in actual notification to those individuals, if the agency has the information available:
   a. In writing, sent to the most recent address for the individual as reflected in the records of the agency;
   b. By electronic mail, sent to the most recent electronic mail address for the individual as reflected in the records of the agency, unless the individual has communicated to the agency in writing that they do not want email notification; or
   c. By telephone, to the most recent telephone number for the individual as reflected in the records of the agency.

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

1. To the extent possible, a description of the categories of information that were subject to the security breach, including the elements of personal information that were or were believed to be acquired;
2. Contact information for the notifying agency, including the address, telephone number, and toll-free number if a toll-free number is maintained;
3. A description of the general acts of the agency, excluding disclosure of defenses used for the protection of information, to protect the personal information from further security breach; and
4. The toll-free numbers, addresses, and Web site addresses, along with a statement that the individual can obtain information from the following sources about steps the individual may take to avoid identity theft, for:
   a. The major consumer credit reporting agencies;
   b. The Federal Trade Commission; and
   c. The Office of the Kentucky Attorney General.

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

(3) (a) The notices required by subsection (1) of this section shall not be made if, after consultation with a law enforcement agency, the agency receives a written request from a law enforcement agency for a delay in notification because the notice may impede a criminal investigation. The written request may apply to some or all of the required notifications, as specified in the written request from the law enforcement agency. Upon written notification from the law enforcement agency that the criminal investigation has been completed, or that the sending of the required notifications will no longer impede a criminal investigation, the agency shall send the notices required by subsection (1)(b)1. of this section.

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

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

(5) This section shall not apply to:

(a) Personal information that has been redacted;

(b) Personal information disclosed to a federal, state, or local government entity, including a law enforcement agency or court, or their agents,

assigns, employees, or subcontractors, to investigate or conduct criminal investigations and arrests or delinquent tax assessments, or to perform any other statutory duties and responsibilities;

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

(d) Personal information that an individual has consented to have publicly disseminated or listed; or

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

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

Effective: January 1, 2015

History: Created 2014 Ky. Acts ch. 74, sec. 3, effective January 1, 2015.

Legislative Research Commission Note (1/1/2015). 2014 Ky. Acts ch. 74, sec. 10 provided that "the provisions of this Act shall not impact the provisions of KRS 61.870 to 61.884." That proviso applies to this statute as created in Section 3 of that Act.

Legislative Research Commission Note (1/1/2015). In codification, the Reviser of Statutes has corrected a manifest clerical or typographical error in subsection (1)(a)1. of this statute by changing a reference to the educational entity agencies that must notify the president of the Council on Postsecondary Education of a security breach that are listed in "subsection (1)(c) of Section 1 of this Act" (KRS 61.931) to "subsection (1)(e) of Section 1 of this Act," making the reference once codified read "KRS 61.931(1)(e)."

Legislative Research Commission Note (1/1/2015). In codification, the Reviser of Statutes has corrected a manifest clerical or typographical error in subsection (1)(a)2. of this statute by changing a reference to the security and breach investigation procedures and practices referenced in "subsection (1)(b) of this section" to "subsection (1)(b) of Section 2 of this Act," making the reference once codified read "KRS 61.932(1)(b)."