New Security Requirements for Personal Information Held by Water Districts

On March 31, 2014, the General Assembly enacted House Bill 5. Governor Beshear signed the bill into law on April 10, 2014. House Bill 5 generally requires state and local government agencies to implement and maintain procedures to protect against security breaches; to disclose security breaches to designated state officers; to investigate potential security breaches, and to notify designated state officers and affected members of public when breach is likely to result in misuse of personal information.

Applicability. House Bill 5 applies to all Executive Branch Agencies, cities and their boards and agencies, counties and their boards and agencies; special purpose governmental entities (includes **water districts**) that maintain or otherwise possess personal information.

What is Personal Information? "Personal information" means an individual's first name or first initial and last name; personal mark; or unique biometric or genetic print or image, in combination with

- An account number, credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an account;
- A Social Security number;
- A taxpayer identification number that incorporates a Social Security number;
- A driver's license number, state identification card number, or other individual identification number issued by any agency;
- A passport number or other identification number issued by the United States government; or
- Individually identifiable health information

The form in which the personal information is maintained is irrelevant – it may be in physical or electronic medium.

Development of Procedures and Practices to Protect Against Security Breach. If a water district possesses personal information, it must develop, maintain, and update procedures and practices, including taking protective action to protect against security breaches. Its security investigation and breach procedures must be consistent with Department of Local Government's (DLG) policies and must be in place no later than January 1, 2015.

What is a Security Breach? A "security breach" is the unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that compromises or that the agency or nonaffiliated third party reasonably believes may compromise the security, confidentiality, or integrity of personal information and result in the likelihood of harm to one or more individuals.

Can a Security Breach involving encrypted records occur? Yes. A security breach occurs if, unauthorized acquisition or release of the confidential process or key to unencrypt the records or data occurs. Unauthorized release or acquisition of encrypted data does not constitute a security breach unless the key is also released or acquired.

Procedures in event of Security Breach. Within 72 hours of notice or determination of a security breach, a water district must notify the Kentucky State Police, Auditor of Public Accounts, the Attorney General and the DLG Commissioner and begin an investigation in accordance with its security and breach investigation procedures. Within 48 hours of the investigation's completion, the water district must notify Kentucky State Police, Auditor of Public Accounts, Attorney General, Commissioner of Department of Libraries and Archives, and the DLG Commissioner.

Notification of Persons Affected by the Security Breach. Within 35 days after notifying the required officials of the results of the investigation, Water District must notify all persons affected by breach if it determines that misuse of the personal information has occurred or is likely to occur. If more than 1,000 persons must be notified, water district must at least 7 days prior to the issuance of notification notify DLG and consumer reporting agencies regarding timing, distribution, and content of notice. Notification will only be made after consultation with law enforcement and will be delayed if the water district receives a written request from law enforcement stating that notification will impede investigation. Notification may also be delayed if the delay is necessary to restore the reasonable integrity of system and the Attorney General approves of delay in writing.

Method of Notification. A water district must notify persons affected by a security breach by: (1) Posting a notice conspicuously on its website; (2) Notifying regional or local media; or (3) Providing notification by mail, e-mail, or telephone. The method used must be the most likely to result in actual notification.

Form of Notice. The notice must be clear and conspicuous; contain a description of the categories of information breached; provide the water district's contact information including address and telephone; contain a description of the water district's actions to protect information from further disclosure; and contain the toll-free telephone numbers, addresses and website addresses for the major credit reporting bureaus, Federal Trade Commission, and the Office of Kentucky Attorney General.

Circumstances When No Notification Required. If the water district determines after an investigation that no misuse has occurred or is likely to occur from the breach, then no notification to the public is required. The water district, however, must maintain records that reflect the basis for its decision and must notify the Kentucky State Police, the Auditor of Public Accounts, the Attorney General and the DLG Commissioner of the results of its investigation.

Non-Affiliated Third Parties (NTPs). An NTP is any person that has a contract or agreement with an agency and receives personal information from the agency as a result of that contract. Examples of possible NTPs include health insurance carriers, attorneys, accountants, and information technology contractors.

Duties of NTPs. Any NTP that obtains personal information from a water district or collects personal information on behalf of a water district must:

- Implement, maintain, and update appropriate security and breach investigation procedures that are at least as stringent as the investigation procedures and practices that the water district must follow.

- Notify the water district within 72 hours of determination of a security breach of the personal information within the NTP's possession and provide all information that it has at the time of notification regarding the breach.

Contracts with NTPs. Any agreement between a water district and an NTP under which the water district discloses personal information to the NTP and which is executed or amended after January 1, 2015, must require the NTP to implement, maintain, and update appropriate security and breach investigation procedures and must specify how the costs of the notification and investigation requirements are to be apportioned when a security breach is suffered by the NTP.

Enforcement. The Attorney General is authorized to enforce the provisions of House Bill 5.

Private Right of Action. House Bill 5does not create a private right of action to enforce the provisions of the Bill or seek damages or penalties for failure to comply with the Bill's provisions. However, a water district customer who claims harm due to the water district's security failures is not necessarily barred from suing a water district for negligence after a breach. Kentucky Courts have not yet addressed whether governmental immunity would protect a water district from such legal actions.

Prepared By:

Gerald E. Wuetcher
Stoll Keenon Ogden PLLC
859-231-3000 (office)
859-231-3017 (direct)
859-550-3894 (cell)
300 West Vine St. Suite 2100
Lexington, KY 40507-1801
gerald.wuetcher@skofirm.com
https://twitter.com/gwuetcher

Date: November 20, 2014