A PRIMER ON KENTUCKY’S
DATA BREACH NOTIFICATION LAW

By: Patrick H. Haggerty

Data breaches continue to dominate the news, with companies such as Target, Home Depot, Sony Pictures Entertainment, eBay, and Anthem reporting incidents affecting millions of customers and employees. No company is immune. And it is not just payment cards or health care information at risk—employee data, intellectual property, and business sensitive data is also being taken. Between 2005 and March 20, 2015, there have been 5,203 breaches exposing more than 778 million records, according to the Identity Theft Resource Center. In 2014 alone, the Privacy Rights Clearinghouse estimated that over 67.5 million records were affected as a result of 295 publicly-known security breaches caused by unintended disclosures, hacking or malware, payment card fraud, persons with legitimate access, or lost or stolen paper documents or devices.

Depending on the incident and data at risk, affected individuals may face an increased risk of fraud or identity theft. According to a study conducted by the National Consumer League and Javelin Strategy & Research in July 2014, affected individuals face a one-in-three chance of becoming a victim of identity fraud. The consequences of a breach for an organization also can be significant, and may include lawsuits, government investigations, adverse media attention, business disruption, and reputational damage. According to a May 2014 study by IBM and the Ponemon Institute, the average cost of a data breach for an organization was $5.85 million and the average cost for each lost or stolen record was $201.

There is currently no national standard for data breach notification. Existing federal laws governing data breach notification are limited to specific sectors such as financial institutions (e.g., the Gramm-Leach-Bliley Act (“GLBA”)) and healthcare (e.g., Health Insurance Portability and Accountability Act (“HIPAA”)). With no national data breach disclosure law on the books, companies are forced to adhere to a patchwork of state laws. State data breach notification laws are designed to help protect individuals whose data has been compromised by providing timely notice to all affected individuals. By receiving timely notice, affected individuals can take steps to protect themselves against the potential consequences of a data breach, which could include identity theft or fraud. State laws, however, vary in terms of who must comply, the definition of personal information, what constitutes a breach and notification requirements.

Prior to 2014, Kentucky was one of only four states—including Alabama, New Mexico, and South Dakota—that did not have a data breach notification law. This changed when the Kentucky legislature passed and Governor Beshear signed H.B. 232 into law, making Kentucky the 47th state to enact a data breach notification law. The law became effective July 15, 2014.

Companies now hold vast amounts of personal information about individuals. Once an individual’s personal information is breached, it is difficult for a company to retrieve and secure what has been lost. Recognizing the reality of data breaches and the potential harmful effects, the Kentucky legislature has instituted a statutory scheme to prevent the main threat caused by data breaches, namely, identity theft. All companies must be aware of Kentucky’s data breach notification law, and be ready to comply with its requirements.

What entities/persons are covered? The law applies to an “information holder,” which is defined as any person or entity that conducts business in Kentucky. The law does not apply to any person or entity subject to HIPAA and GLBA. The law also does not apply to any agency of the Commonwealth or any of its local governments or political subdivisions. There is a separate breach notification law applicable to any agency of...
the Commonwealth and nonaffiliated third parties," which includes "any person that (a) [h]as a contract or agreement with an agency; and (b) [r]eceives personal information from the agency pursuant to the contract or agreement."19

What information is covered? The law covers "personally identifiable information," which is defined as "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or data element is not redacted: (1) Social Security number; (2) Driver's license number; or (3) Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account."10 The law only applies to unencrypted and unredacted computerized data—it does not apply to paper records.11

The law defines a "breach of the security of the system" as the "unauthorized acquisition of unencrypted and unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder as part of a database regarding multiple individuals that actually causes, or leads the information holder to reasonably believe has caused or will cause, identity theft or fraud against any resident of the Commonwealth of Kentucky."12 Upon notification or discovery of a breach of the security of the system, an information holder must notify "any resident of Kentucky whose unencrypted information was, or is reasonably believed to have been, acquired by an unauthorized person."13

When must affected individuals be notified? Notifications to affected individuals must be "made in the most expedient time possible and without unreasonable delay."14 The law allows the information holder to take into account the "legitimate needs of law enforcement … [and] any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system… [and] notification… may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation."15 The law requires that the individual or entity promptly notify the affected individuals once the law enforcement agency determines the investigation will not be compromised by notification.16

How must notice to affected individuals take place and what must it include? Notice may be provided in writing (e.g., on paper and sent by mail) or in electronic form (e.g., by e-mail but only in compliance with the federal Electronic Signatures in Global and National Commerce Act ("E-SIGN").17 Under E-SIGN, sending a breach notification notice to an individual in electronic form is acceptable only if the individual affirmatively consents to receive an electronic notice in lieu of a paper notice, provides such consent electronically, and does so in a manner that "reasonably demonstrates" that he or she can access the electronic information in the form that will be used.18 Moreover, prior to consenting, the individual must be provided with a clear and conspicuous notice that informs the consumer of: (1) his/her option to have the information provided on paper; (2) the procedures the individual must use to update information needed to contact the consumer electronically; (3) how, after consent to electronic notification, he/she may obtain a paper copy of the electronic notice, and the fee therefore; (4) the hardware and software requirements for access and retention of the electronic notice; (5) his/her option to withdraw consent to electronic notification, and the procedures the individual must use to withdraw consent; and (6) the conditions, consequences, and fees of withdrawing such consent.19

If the information holder has "notification procedures as part of an information security policy for the treatment of personally identifiable information, and is otherwise consistent with [the law's] timing requirements …, [the information holder] shall be deemed to be in compliance with [the law's] notification requirements …, if it notifies [affected individuals] in accordance with its policies…."20 The law does not contain any specific notification letter content requirements.

Can substitute notice be provided to affected individuals? Notification can be provided via substitute notice if the information holder can demonstrate the number of individuals to be notified exceeds 500,000, the cost of providing notice would exceed $250,000, or a lack of sufficient contact in-
formation for those affected. Substitution notice must consist of all of the following: (1) e-mail notice, when the information holder has an e-mail address for the affected individuals, (2) conspicuous posting of the notice on the information holder's website if the information holder has a website; and (3) "[n]otification to major statewide media." Do information holders need to notify the credit reporting agencies? If the information holder discovers circumstances which require notification to greater than 1,000 persons at a time, consumer reporting agencies are to be notified, without unreasonably delay, "of the timing, distribution, and content of the notices." Do information holders need to notify the Kentucky Attorney General of a security breach? The law does not require notification to the Kentucky Attorney General or any other state regulatory authority. What happens if the information holder does not own the personally identifiable information (i.e., a vendor)? The law requires that "[a]ny information holder that maintains computerized data that includes personally identifiable information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data as soon as reasonably practicable following discovery, if the personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person." What happens if a person or entity fails to comply with the breach notification law? The statute itself is silent as to any penalties for noncompliance as well as whether a private right of action exists under the statute. In addition to knowing the requirement of the law, there are number of measures a company can take to successfully prepare for a data breach and become "Compro-mise Ready": Carefully select an intelligent and capable incident response team. An incident response team is a carefully selected and well-trained group of people whose purpose is to promptly and correctly handle an incident so that it can be quickly contained, investigated, and recovered from. Creating a compact, intelligent and well-trained incident response team is crucial to being prepared to handle any incident, large or small, which a company may face. An incident response team is usually comprised of members from within the company and usually includes the following individuals (or their equivalents in the company structure): the chief information security officer, chief information officer, chief corporate governance officer, assistant chief operating officer, director of security and chief administrative officer. The team should be able to provide a measured and thorough response, appropriate to the determined seriousness of the breach. Develop a comprehensive incident response plan. Time is of the essence in responding to a data breach. By having an incident response plan in place, companies can best position themselves to respond quickly after learning of a data breach. An incident response plan is intended to provide an organized approach for responding to potential threats to the confidentiality, integrity, or availability of a company's information technology or data. The plan should be designed to enable: (1) prompt identification and containment of security incidents; (2) remediation of any identified vulnerabilities; (3) prevention of disruption of critical information systems; and (4) assessment of what occurred, notification of affected individuals and regulators as necessary, and mitigation of consequences that may arise from any unauthorized access. The plan should be sufficiently general to cover a wide range of potential incidents without containing too much detail or too many steps that might be considered too complex for a team to easily execute under pressure. Identify external service providers. As part of developing an incident response plan, companies should identify the third parties they may need to bring onboard to assist in responding to a potential incident, including legal counsel with privacy and security experience, a forensic investigation firm, a crisis communications firm, a company to provide credit monitoring services, and a vendor who can help mail notification letters and operate a call center. Conduct tabletop exercises. Having an incident response team and plan is a first step towards being ready for an incident, but having a plan in a binder on a shelf and a team assembled is not enough. Companies who test their plans consistently through tabletop exercises using realistic mock breach scenarios improve their plans and, equally important, train their incident response team in the process. An incident response team must learn not to act too quickly or reveal too much information to the public too soon. A thorough forensic analysis and investigation of the incident must be completed before going public, as not every cyber security incident results in a data breach. Systems may be hacked, but data might not be exfiltrated. Stolen laptops may be recovered before confidential information is accessed. Acting hastily could cause unnecessary public alarm and otherwise avoidable reputational damage. The proper training teaches the team to act in a calm, organized and careful manner. With careful and thoughtful planning, companies can be prepared to respond to an incident in a manner that complies with the law and protects their reputation and customer relationships.