Published on *The National Law Review* https://natlawreview.com

Businesses, Take Note of New Breach Notification Duty

Article By:

McBrayer, McGinnis, Leslie & Kirkland, PLLC

Kentucky just became the 47th state to enact **breach notification legislation**. For businesses, that means that there is a now a legal obligation to **inform customers** when a **data breach** occurs that could leave them vulnerable to identify theft. No business's security system is safe from hackers. You may recall that in January 2014, Target reported that between 70 to 110 million of its customers had personal information stolen in a widespread data breach during the holiday season. Data breaches, whether big or small, can leave customers exposed to fraudulent activity and cause massive reputational damage to businesses.

Pursuant to House Bill 232's provisions, a security breach is defined as "the unauthorized acquisition of unencrypted, unredacted computerized data that compromises the security, confidentiality, or integrity of personally identifiable information maintained by the information holder [i.e., business] as part of a database regarding multiple individuals that causes or leads the information holder to believe has caused or will cause identity theft or fraud against a Kentucky resident."

"Personally identifiable information" includes an individual's first name or first initial and last name in combination with one or more of the following unredacted data elements: (1) Social Security number; (2) driver's license number; or (3) account number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Upon notice or discovery that a security breach has occurred, a business must inform Kentucky residents of the breach "in the most expedient time possible and without unreasonable delay," consistent with 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.

Notification can be carried out in several ways:

(a) Written notice;

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

(c) Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to

be notified exceeds five hundred thousand (500,000), or the information holder does not have sufficient contact information. Substitute notice shall consist of all of the following:

1. E-mail notice, when the information holder has an e-mail address for the subject persons;

2. Conspicuous posting of the notice on the information holder's Internet Web site page, if the information holder maintains a Web site page; and

3. Notification to major statewide media.

In the event that a large-scale data breach occurs, requiring notification of more than 1,000 persons at one time, consumer reporting agencies must be notified without unreasonably delay.

The provisions in House Bill 232 do not apply to any person or entity subject to Title V of the Gramm-Leach-Bliley Act, any person or entity subject to HIPAA, or any Kentucky agencies, local governments, or political subdivisions. Further, a business that maintains its own notification procedures as part of an information security policy may be deemed compliant with House Bill 232, as long as the policy's timing requirements are consistent with those established in the bill and affected residents are notified in accordance with the policy.

National Law Review, Volume IV, Number 122