

# Kentucky Becomes 47th State With Data Breach Notification Law

APRIL 14, 2014

Kentucky has become the latest state to [pass a breach notification law](#), which will become effective this July. Starting then, companies that hold information about Kentucky residents and who suffer a data breach—defined in that state as an unauthorized acquisition of “unencrypted and unredacted computerized data” that compromises the security of that data or is likely to lead to identity theft—will now be required to notify state residents. Data that triggers the laws’ requirements (if breached) is name and social security number, driver’s license number, or account number/credit card number in combination with any required security code to permit access to a person’s financial account. Notification to impacted individuals can be delayed if a law enforcement agency determines that it would “impede a criminal investigation.” Given that almost every state, as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands already have a breach notification statute in place, with almost identical provisions, this new law will likely change little for national corporations, especially as it contains no requirement to notify state authorities.

**TIP: Companies that already have breach notification procedures in place, and who have a practice of notifying all impacted individuals in the event of a nationwide breach, will not likely be impacted by this new Kentucky law.**

1 Min Read

## Related Locations

Chicago

## Related Topics

Data Breach

## Related Capabilities

*This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.*