How prevalent are data breaches in the United States?
In 2014, 1,343 breaches occurred in the United States, exposing 512 million records, which is an increase from previous years. For instance, more than 600 breaches occurred in 2009 and 1,054 in 2013.

How many states have adopted breach notification laws?
Forty-seven states and the federal government have adopted some form of law that requires organizations sustaining a breach to disclose the incident and notify consumers if their data were exposed.

Are these laws effective?
Some research has shown that notification laws can reduce the rate of identity theft, but oversight might be needed to encourage compliance. What information organizations disclose to consumers after a breach may also be important to consumer protection.

What provisions within these laws help protect consumers?
Data breach notification laws enable victims to take actions to protect against identity theft, but provisions within notification laws may vary in how effectively they provide this opportunity. We evaluate a state’s effectiveness in deterring identity theft by the provisions provided in that particular state’s law. We found states that included the “State Enforcement” provision, which allows the attorney general or another designated state entity to enforce organizations’ failure to comply with the statute, had fewer incidents of identity theft than states that did not include the provision. Another effective provision was “Explicit Time Limit to Notify,” which requires organizations to notify affected customers within a given number of days, usually 30 or 45 days as opposed to the vague requirement, or as quickly as possible and without unreasonable delay.

Where there provisions that increased the risk of identity theft?
We found three provisions associated with higher identity theft. Two of these provisions, Risk of Harm and Baseline Encryption Exemption, could make it easier for organizations to legally avoid disclosing a data breach. If an organization misinterprets the risk of harm from a breach and chooses not to notify victims, then preventable identity theft may occur. Likewise, if an organization with a weak encryption system does not notify victims, then the breach’s perpetrators may be able to decrypt the stolen data and consequently steal identities.