

No Business Too Small to Ignore Data Security Breaches

August 2014

Vermont Attorney General William Sorrell made some waves in early July by bringing an enforcement action against a small country store for failing to comply with that state's breach notification law. The takeaway is that there is no "too small" exception to data security. Breach notification laws apply to businesses that are quite small, just as they do to the Targets and TJ Maxx's of the world.

Breach Incident

The e-commerce website of the Shelburne Country Store was hacked in November 2013, compromising the credit card information of more than 700 customers. Upon learning of the breach, the store fixed the problem. However, Vermont's data security breach notification law required it to report the breach to the state attorney general's office and to notify the affected customers. It did neither.

Although the store claimed that it was unaware of the obligations, the Vermont AG stated that no business should be unaware of them given the publicity garnered by security breaches at large retailers around the nation. Of course, ignorance of the law is no excuse. Ultimately, the store agreed to pay a small \$3,000 fine. Perhaps more importantly, it also agreed to establish a comprehensive information security program and to comply with the Payment Card Industry data security standards. One could reasonably argue that both of these two latter steps were already required either by law or by contract.

Implications for You

What does this mean for you? First, there is no "small business" exception to state data breach notification laws. A victim of identity theft likely cares little whether the source of the data breach was a large national retail chain or a small family store.

Second, all companies have obligations to maintain the security of customer payment information, and employee financial data as well. What security measures are appropriate will depend upon the types of data that are stored, the reasonably foreseeable risks and threats, and what is commercially reasonable under the circumstances. What small businesses cannot do is simply assume that such obligations somehow do not apply to them.