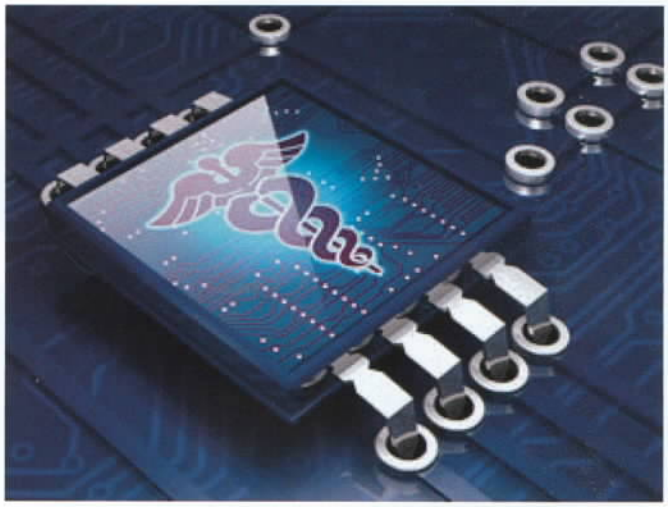
damages they sustain as a result of the data breach. However, the bad news is that your company and your clients have hundreds of employees who reside in those 11 jurisdictions.

Seeing dollar signs fly by, you ask what the risk would be of not notifying anybody; in the hope the information is never wrongly used. You learn that several state statutes impose fines ranging from $10,000.00 to $150,000.00 per breach if required notification is not made. Other jurisdictions impose civil penalties or fines up to a $500,000.00. Not notifying all those entitled to notification simply is not an option.

"I thought all the laptop computers you gave to your employees had encryption, GPS location and remote destruction software," your lawyer says. You respond that, in an effort to save hardware costs and address concerns of a new generation of "techies" who want to do all their computing on a single device, your company recently adopted a BYOD policy that allows employees to use a single device of their own choosing for both personal and company business. You did not require employees using personal devices to download those protective software programs. Your lawyer asks what steps you took to protect the company's own trade secrets and confidential information on employee devices. You never thought about that and have no protection either from whoever stole the computer or even from your own employees' wrongful use of that information.

Your lawyer advises that, because there is health information on the laptop subject to HIPAA and HITECH, you are subject to an enforcement action by Health and Human Services. He also advises that under the Interagency Guidance Publication issued by the Comptroller of Currency under Gramm-Leach-Bliley your company was required to have in place a risk-based response program to address incidents of unauthorized



access to private information because your business qualifies as a financial institution under the Financial Services Modernization Act of 1999.

You belatedly realize that, before adopting a BYOD program, you should have completed a comprehensive risk assessment. Such an assessment might have revealed that employees already were using their own devices for work related information and likely would have determined whether a BYOD program was technically or financially feasible and appropriate for your company. Such an assessment also would have enabled you to select the best technological means for implementation of a comprehensive security program and to develop specific policies and procedures governing BYOD administration and management.

Your lawyer recommends that, after this crisis is over, the company develop a comprehensive BYOD risk assessment procedure and urges you to contact your Errors and Omissions carrier to determine whether you have coverage in the event your clients, their employees or your own employees bring damage lawsuits.

Although fictional, the foregoing arises out of actual events. ■