Is There Automatic Civil Liability For A Data Breach?

Insights
11.14.17

No! It is a common misconception among the general public that someone always has to pay when there is a data breach. It is understandable that individuals affected by a data breach will be upset, distraught, and even angry. In light of recent large-scale data breaches, it is safe to say we have all been there, with our personal information that we entrusted to particular companies or employers now out there in the hands of cyber thieves.

Data breaches may result in serious harm to the affected individuals, such as identity theft and disruption of their lives and businesses. Of course they will want someone to pay, and they will probably find a plaintiffs' attorney who will file a lawsuit regardless of whether your company has any liability, hoping that a jury would reward the "victim" simply because they suffered damages.

The reality is that data breaches happen to the best of us. And sometimes even if a company took every reasonable step within its power to prevent data breaches and ramp up security, it may still experience a data breach. But the accusations will still be made: "How could you let this happen?" "I trusted you to keep my data secure." "You're going to pay!" It is common for individuals affected by a breach to believe that a data breach could not have possibly occurred without someone being negligent. This common reaction results in a high propensity for litigiousness among the victims of any data breach.

Laws Provide Some Breathing Room For Diligent Companies
Generally, data privacy laws across the United States, both state and federal, do not impose strict civil liability on entities that experience a breach of security resulting in the disclosure of personal information to unauthorized or unknown parties. Rather, potential civil liability may arise in two scenarios. First, if a company fails to implement steps that are either required by statute or reasonable under the circumstances to safeguard private information, it could face the very real possibility of a negative legal judgment. Second, even if a company implemented legally required or reasonable steps to prevent a breach before it occurs – in other words, did everything right up to the breach incident – it could still face liability if it fails to take post-breach steps to remedy the situation or mitigate the harm. This could include steps required by a specific state statute, such as providing notification to those impacted, or those simply deemed reasonable under the unique circumstances related to the specific breach in question.

While statistics show that most data breaches have a root cause of human error, a human error does not automatically mean the company was negligent. A legal determination of fault under a

not automatically mean the company was negligent. A legal determination of fault under a negligence theory will depend on the precise circumstances in which the mistake or human error was made. This is also the case if the breach was the result of intentional or malicious actions by an insider. Unfortunately, the lawyerly answer "it depends" still applies.

Nightmare Hypothetical Scenario Demonstrates Potential Problems

For example, imagine a rogue and disloyal employee bent on misappropriating your trade secrets defects to a competitor after uploading electronic files pertaining to your customers and employees to their Google Drive (in an attempt to bypass USB detection). It turns out the files contain private non-public information of customers and medical information of employees. The former employee's Google Drive is then hacked by some unknown party and all the customers' and employees' private information is exposed. Once the affected individuals learn that their information has been leaked, they want someone to pay. Are you at fault for the data breach in this hypothetical scenario?

Ultimately, if you took all the legally required or reasonable steps to safeguard private information, and the data breach occurred despite your best efforts, there should be no liability absent a contractual indemnification or guaranteeship obligation towards the affected individuals. The challenge, however, is proving that you did all you could to prevent a data breach. It may come down to a battle of the expert witnesses opining on what were the applicable "best practices" at the time of the incident. For instance, was it reasonable for the rogue employee to have had access to those files? Was it reasonable for this employee to have been able to access a personal cloud-based account using a company device?

After The Breach: Picking Up The Pieces

Once a breach occurs, a new set of obligations arise, including compliance with applicable state and federal data breach notification laws, some of which may also require the provision of identity theft protection or monitoring services to the affected individuals. When an incident qualifies as a data breach under a state's data breach notification statute, failure to timely notify the affected individuals may give rise to liability for civil penalties imposed by the state's attorney general or other state enforcement authority.

Some statutes create a private right of action so that, in addition to other claims under the common law, the affected individuals may file their own lawsuit for failure to comply with the state's data breach notification law. In the absence of a private cause of action provision in the statute, only the government can enforce and impose penalties for these statutory violations. Of course, this will not stop plaintiffs' attorneys from asserting a common law negligence claim based on violation of the breach notification statute.

In addition to complying with statutes and regulations, companies that experience a data breach of their systems should take steps consistent with their duty of care to the affected individuals. This may potentially include providing identity theft protection services even where not required by law, or extending such coverage for two years where the law only requires one year of coverage. Another reasonable step recommended by data security practitioners is to engage an external, independent security consultant to conduct a comprehensive security assessment or audit of your IT

security consultant to conduct a comprehensive security assessment or audit of your IT infrastructure and information management systems. If the security audit reveals gaps in security, you should promptly take action to implement recommended changes aimed at preventing data breaches in the future.

Related People

Usama Kahf, CIPP/US
Partner
949.798.2118
Email