Court Rules that Sloppy Cyber-security Standards Expose Companies to FTC Enforcement Actions

August 25, 2015 â€“ Three years ago, Wyndham Hotels was ordered by the FTC to pay fines over what the agency deemed to be substandard computer security standards. The agency alleged that Wyndhamâ€™s lax standards for storing customer data were a root cause of two data breaches at the company which led to millions of dollars of fraud losses.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

Wyndham sued. The company claimed that the FTC had no clear authority to set data security standards for companies that store personally identifiable information on their customers. They also claimed that the FTC hadnâ€™t developed a set of security standards for companies to follow; making it nearly impossible to know what the standard was to avoid government fines.

Wyndham lost their initial case so the company appealed. Yesterday, they lost again when the US Third Circuit Court of Appeals ruled against the company.

Wyndham has not said if it will appeal the newest ruling, but the companyâ€™s options are currently limited. It can ask the Appeals Court to rehear the case en banc or it can appeal the ruling to the US Supreme Court. But there is no reason to think that either of these appeal routes would be granted.

The case is significant because it means that companies are now subject to an unpublished data security standard that is to be determined by the FTC.

In some cases, enforcement may be fairly straight forward. For instance, in Wyndhamâ€™s case, the company was accused of not using firewalls to keep intruders out, not using encryption and granting access to company systems using easy to crack passwords.

But in other cases, it may not be so straightforward. For instance, if a company upgrades its firewall to the latest and greatest technology today, if a newer and better firewall becomes available in two months does the company need to purchase it right away or can they continue to use their existing technology for the next year or two? Itâ€™s an important question without an answer right now.

Making changes to the technology that companies use may sound simple but it isnâ€™t. Large organizations need time to test new equipment and code to make sure that it is compatible with their other systems. These tests can take months to complete. And when completed, major changes can result in millions of dollars in expenditures.

For the time being, companies should probably be turning to attorneys who specialize in both technology and government enforcement. Those attorneys should be used to determine the best course of action to take to avoid any future problems with the FTC. Given yesterdayâ€™s court ruling, it is a pretty safe bet that the FTC will step up its cyber-security enforcement actions now that it knows that the courts are on the side of the government.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS