WINSTON & STRAWN LLP

BLOG

Wyndham-FTC Settlement Requires Security Program and Audits

DECEMBER 15, 2015

Wyndham Worldwide recently settled with the Federal Trade Commission in an ongoing data breach and security lawsuit regarding at least three security incidents at Wyndham brand hotels between April 2008 and January 2010. This settlement follows decisions we previously reported on that affirmed the FTC's authority to take enforcement action against private companies for unfair or deceptive data security practices under Section 5 of the FTC Act.

The terms of the settlement agreement will require Wyndham, for a period of 20 years, to establish and maintain a comprehensive information security program reasonably designed to maintain the security, confidentiality, and integrity of consumer cardholder data. The program must include, among other things, designating a person responsible for the program, evaluating and addressing risks, ensuring that service provides adhere to the same safeguards as those implemented by Wyndham, and obtaining annual information security audits.

While these provisions mirror other terms the FTC has reached with companies, there are also some unique provisions. Because of the nature of the Wyndham security incidents, the settlement focused on payment card holder data in particular. Wyndham will be required to obtain annual written PCI compliance assessments by an independent auditor, and if it experiences a data breach involving 10,000 or more unique payment card numbers, Wyndham must tell the FTC about it 190 days after discovering the breach. Specifically, 180 days after discovering the breach, Wyndham must obtain an incident report by a PCI Forensic Investigator and give report to the FTC within 10 days of receiving it.

TIP: This settlement underscores the seriousness with which the FTC takes its regulatory authority in the privacy space. While the FTC has not set out express data security standards, this settlement suggests that the FTC expects companies to have written security programs, a person in charge of privacy and security, and to conduct annual audits and assessments.

1 Min Read

Related Locations

Chicago

Related Topics

Data Breach | Consumer Privacy

Related Capabilities

Privacy & Data Security

Related Regions

North America

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.