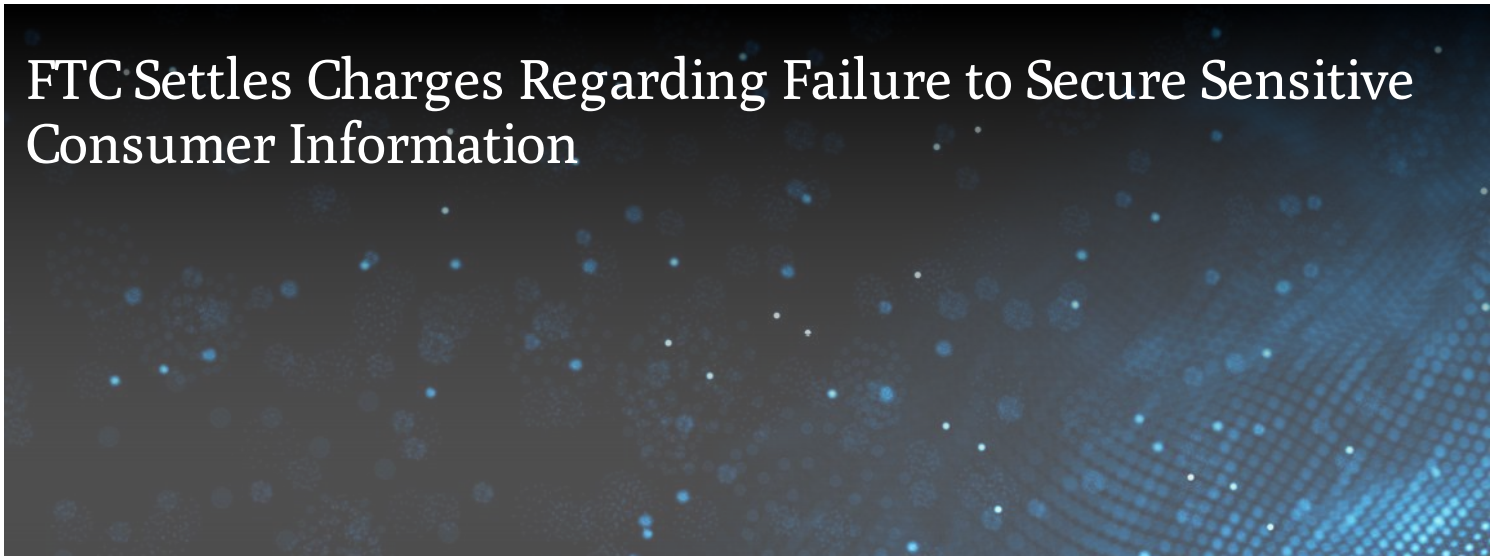
WINSTON & STRAWN LLP

BLOG

FTC Settles Charges Regarding Failure to Secure Sensitive Consumer Information



JULY 3, 2013

The Federal Trade Commission approved a final settlement with HTC America Inc. regarding charges that HTC America failed to adequately secure its mobile software, which placed sensitive consumer information at risk. The FTC alleged that when HTC America customized its Android mobile devices, it failed to employ reasonable and appropriate security in the design. The FTC alleged that HTC America: (a) failed to implement an adequate program to assess the security of products it shipped to consumers; (b) failed to implement adequate privacy and security guidance or training for its engineering staff; (c) failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices; (d) failed to follow well known and commonly-accepted secure programming practices, including secure practices that were expressly described in the operating system's guides for manufacturers and developers, which would have ensured that applications only had access to users' information with their consent; and (e) failed to implement a process for receiving and addressing security vulnerability reports from third-party researchers, academics or other members of the public, thereby delaying its opportunity to correct discovered vulnerabilities or respond to reported incidents. In its complaint, the FTC further identified several other vulnerabilities that it believed HTC America could have avoided by taking reasonable steps to assess the vulnerabilities and security risks present in its mobile devices. Finally, the FTC alleged that the user manuals associated with such devices contained false or misleading statements regarding when user information was accessed or transmitted, including statements that user authorization was necessary for a third party application to access user information when such information could be accessed without authorization because of security vulnerabilities and that the user could select to transmit location data along with user error reports, when the location data may have been actually transmitted regardless of user preference. The settlement requires HTC America to establish, implement and maintain a comprehensive security program that will address security risks related to the development and management of new and existing devices and will protect the security, confidential and integrity of consumer information. HTC America is further required to develop security patches to fix certain security vulnerabilities identified by the FTC.

TIP: This case serves as a reminder that when designing or modifying software used in the collection of consumer information, security considerations should be taken into account. This includes, for example, testing software regularly for security vulnerabilities that may expose sensitive consumer information to risk of unauthorized access or use. And, to the extent vulnerabilities are discovered, making sure they are addressed as soon as commercially reasonable based on the extent of the risk.

This tip 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.

2 Min Read

Related Topics

Data Breach

Related Capabilities

Privacy & Data Security

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.