New FTC Settlement and Cal. AG Lawsuit Reflect Continued Focus on Consumer Data Protection

January 31, 2014

Two new actions announced in the past week indicate that federal and state regulators will continue to aggressively enforce data security and consumer protection laws in the wake of recent high profile consumer data breaches.

Today, the FTC announced a settlement with GMR Transcription Services, Inc. ("GMR"), a provider of medical transcription services, along with two company owners, over claims that GMR employed inadequate data security measures that unfairly exposed the personal information of several thousand consumers to the public Internet. According to the FTC, despite GMR's public assurances that data maintained in its system would remain private and secure, a service provider working on behalf of GMR inadvertently allowed consumers' highly sensitive medical information, driver's license numbers, tax information, and other data to be indexed and searchable through a major search engine. Under the settlement, GMR is prohibited from misrepresenting the extent of its privacy safeguards. The company also must establish a comprehensive data security program that will be subject to biennial independent audits for the next 20 years.

On January 24, California Attorney General Kamala Harris filed a lawsuit against Kaiser Foundation Health Plan ("Kaiser") for failing to provide its employees with timely notice following a data breach that occurred in September 2011. California's breach notification law requires that entities provide notice "in the most expedient time possible and without unreasonable delay" following a breach. According to the complaint, Kaiser did not notify affected individuals until March 2012, after completing a forensic investigation into the breach two months earlier. The complaint also alleges that, in conjunction with the data breach, Kaiser violated a California law that prohibits the "public posting" of social security numbers. The numbers were allegedly "publicly posted" because they were stored on an unencrypted hard drive that was later sold at a thrift store in Santa Cruz, CA.

These latest actions serve as a reminder to companies of their obligations both when collecting and storing consumer information and when responding to a data breach.