SpencerFane®

# FTC Provides a Wake-Up Call for Companies with Lax Privacy Policy Compliance

How confident are you that your website privacy policy accurately explains what you're doing with your customer's data? You now have another 1,500,000 reasons to potentially worry, because the FTC recently slapped GoodRx with a $1.5 million penalty for privacy violations. While this is the first time a regulatory penalty has been handed out under the FTC's Health Breach Notification Rule, more enforcement actions are anticipated. This particular penalty related to the prescription drug discount company GoodRx Holdings Inc. failing to accurately notify consumers of its disclosures of personal health information to Facebook, Google, and other companies.

According to the FTC's complaint, GoodRx shared sensitive personal health information for years with advertising companies, contrary to their promises made in their privacy policies. Among other violations, GoodRx failed to report these unauthorized disclosures which is required under the Health Breach Notification Rule.

The FTC has a history of taking enforcement action against companies who provide misleading information to consumers, including in online privacy policies. Expanded enforcement of online privacy compliance is occurring on a state level as well. For example, in late 2022, the Attorney General for California settled a California Consumer Privacy Act (CCPA) enforcement case against Sephora for $1.2 million in a landmark settlement.

This trend of enforcement actions against businesses for violating data privacy laws should cause all businesses who have an online presence to verify their compliance with applicable law. While historically compliance with online privacy laws was relatively easy, it is becoming more complex as more individual states enact new

data privacy requirements. In addition to California, the following states now have consumer privacy laws that are going into effect this year – Colorado, Connecticut, Virginia, and Utah. A stronger push by government regulators to force compliance "or pay the price" certainly appears to be reality.

The five states that currently have consumer data privacy laws is just the tip of the iceberg. Numerous other states have pending legislation on identical topics. In addition to state and federal regulators, there is an increasing amount of class action litigation brought by plaintiffs' attorneys, particularly under California's law. The bottom line is that companies who overlook consumer privacy compliance may pay far more in the future through penalties and litigation than if they just became compliant with applicable law.

This GoodRx FTC enforcement action is in line with our advice to all businesses that have a website and some sort of online presence. Importantly, it is not enough to simply have a privacy policy that is compliant with the requirements of the law. Instead, a business must adhere to their own policy or face penalties like those mentioned above.

It is important to have an experienced technology team working with you to draft, test, and review a comprehensive privacy policy compliance program. Your technology and marketing teams should work closely with a technology attorney on this work. Combining the knowledge of an experienced technology attorney to go with your employee team's knowledge of operations will allow you to have a comprehensive and compliant privacy policy as well as ensure the customer data privacy practices are being implemented.

So, what should executives and business owners do in light of the current trend of enforcement actions regarding breaches of data privacy laws?

- Review your current privacy policy and confirm with an internal expert that your customer's data is being handled in line with the policy.
- Assuming you have a trusted lawyer, who is experienced in technology and data privacy law, ask them to review your current privacy policies to make sure they are compliant with applicable law, including the new laws taking effect in 2023.
- Assign an individual in the company to "own" the data privacy compliance process.

- Test your company's actual response to some example requests that may come in from consumers.

This blog was drafted by Jack Amaral and Jon Farnsworth, attorneys in the Spencer Fane Minneapolis office. For more information, visit www.spencerfane.com.