Bloomberg Law®

bloombergbna.com

INSIGHT: FTC Has Big Agenda for 2019. How Should Companies Prepare?

BY MICHELLE L. ROGERS AND KATHERINE HALLIDAY

Federal Trade Commission Chairman Joseph Simons recently previewed an aggressive and expansive consumer protection agenda for 2019, invoking the commission's broad powers to pursue unfair or deceptive acts or practices, and adding ''fraudulent'' to the types of conduct he expects to police.

Among the substantive areas of concern are consumer privacy, data security, marketing and, notably, ''policing the financial marketplace,'' a responsibility that has most recently fallen to the Consumer Financial Protection Bureau (CFPB). Simons was clear that the FTC would use all its available tools to protect consumers.

What to Expect

Consumer Privacy and Data Security

Simons devoted significant attention to privacy and data security, which he stated remain a ''top enforcement priority.''

Significant data breaches or reports of lax privacy protections invite FTC investigations. Simons also spoke of the need for legislative fixes, endorsing data security legislation that includes powers to levy civil money penalties and FTC authority to implement the statute.

Financial Marketplace

The FTC will continue with its increasingly active approach to policing financial service providers, with an emphasis on fintech.

Simons cited three recent FTC matters as examples of efforts to ensure that companies fully disclose benefits and risks to consumers. Until recently, the FTC seemed content to leave oversight of financial services providers primarily to the CFPB, which relied on its own UDAAP (unfair, deceptive, and an extra ''A'' representing ''abusive'' acts or practices) authority.

With the CFPB's activity down sharply under the current administration, Simon's remarks suggest the FTC will continue to step up its financial services enforcement, which it can easily do through its own UDAP authority, expertise, and resources.

Advertising

The FTC is assessing the use of influencers, native advertising, and consumer reviews in deceptive advertising, focusing on failures to identify sponsored context and disclose biased relationships.

It will also continue to target deceptive health and safety claims in advertising, particularly those targeting older Americans or touting product efficacy in treating specific conditions.

The FTC is considering additional remedies in advertising enforcement, such as providing notice and remediation to consumers if sales revenue increased significantly due to a company's deceptive claims.

Consumer Fraud

Simons discussed the rise of cryptocurrency and the FTC's initiatives to educate consumers on its risks while simultaneously taking action against deceptive operations.

He also highlighted the FTC's partnership with federal, state, and international law enforcement to shut down scams where fraudsters masquerading as tech

support trick consumers into unnecessary and costly computer repairs.

Simons noted the FTC's efforts to police legitimate businesses that facilitate fraud by ignoring or failing to monitor for red flags.

How to Prepare In response to this aggressive agenda for 2019, companies can and should take proactive steps to stay off the FTC's radar and to ensure that they can defend against unforeseen events by building a strong compliance infrastructure.

Implement a Strong Complaint Management Program

Many of the FTC's initiatives are triggered by consumer complaints, which it tracks through Consumer Sentinel, a nonpublic, online database that aggregates complaints submitted to a wide range of government and private entities—including the CFPB and many state attorneys general—and can be accessed by any federal, state, or local law enforcement agency.

The FTC mines this data to identify trends and repeat offenders; companies can anticipate FTC concerns by developing their own centralized repository to track consumer complaints, uncover trends, and identify issues through root-cause analysis, and by monitoring the FTC's own complaint reporting.

Maintain Strong Data Security and Privacy Policies,Practices

Companies should regularly review their policies and procedures relating to data security and privacy protection to ensure that they are consistent with all applicable laws.

Monitoring technological advances and updating data security strategies will help them adapt to new challenges. Reviews of data and privacy protection protocols should extend to vendors and business partners.

Vet Marketing Materials Thoroughly, Including Social Media

Companies can manage risk through an expansive definition of advertising that includes social media, and indeed, public statements in any forum.

Companies without a social media policy should strongly consider adopting one.

Prioritize Fraud Detection and Reporting

The FTC will not excuse companies that facilitate fraud resulting from insufficient monitoring. Companies should ensure they have the appropriate systems and practices in place to detect, and where applicable, halt potentially fraudulent transactions.

As with data security, companies must be committed to ongoing reviews and enhancements of their fraud capabilities to adapt to technological advances and keep up with the FTC and other regulators' expectations for best practices.

Follow the FTC

Companies should monitor FTC press releases and public statements to gain insight about its enforcement priorities and legislative agenda. It regularly hosts events that are open to the public and are informational.

Author Information *Michelle Rogers is a partner and Katherine Halliday is counsel at Buckley LLP. They represent institutions in a wide range of government enforcement matters involving the FTC, and other state and federal enforcement authorities and regulators, including in investigations, examinations, and litigation.*