The Federal Trade Commission is investigating the data breach of retail giant Target that exposed millions of customers' personal information during the holiday shopping season, raising the possibility the company could face fines and ongoing regulatory scrutiny to prevent future lapses in security.

"We can confirm the existence of an investigation," said an email from Jay Mayfield, FTC spokesman. "We have no further comment on this matter."

Companies including Facebook and Google that have settled customer protection complaints filed by the FTC had to agree to multiyear reviews of their compliance with agency regulations. Target could face a similar fate if the regulator determines the company deceived its customers or ignored their well-being.

[**READ:** Target Data-Theft Victims Become a Credit Agency Gold Mine]

Congress continues to scrutinize Target and other retailers about poor security that allowed hackers to steal more than 40 million payment card records and more than 70 million other customer records. Sen. Richard Blumenthal, D-Conn., asked the FTC to investigate Target in December shortly after the breach was made public.

Adding to the scrutiny is new analysis that Target may have ignored warnings about security gaps and "missed a number of opportunities" to prevent the massive data breach, according to a report published on Wednesday by the Senate Committee on Commerce, Science, and Transportation. Testifying on Wednesday during a hearing of that committee, FTC Chairwoman Edith Ramirez said "a company acts deceptively if it makes materially misleading statements or omissions."

"Further, a company engages in unfair acts or practices if its data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition," Ramirez said in her prepared remarks. "The Commission has settled more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice"

During her remarks, Ramirez supported a national standard for retailers to share information about data breaches but added "there is no one-size-fits-all data security program" and said "the mere fact that a breach occurred does not mean that a company has violated the law."

Sen. John "Jay" Rockefeller, D-W.Va., chairman of the committee, has introduced the Data Security and Breach Notification Act to require the FTC to issue security standards for Target and other companies that manage customer information.

[**ALSO:** Senate, Retailers Push Data-Theft Law]

"I think we can all agree that if Target – or any other company – is going to collect detailed information about its customers, they need to do everything possible to

protect it from identity thieves," Rockefeller said in a news release on Wednesday. "It is increasingly frustrating to me that organizations are resisting the need to invest in their security systems. Target must be a clarion call to businesses, both large and small, that it's time to invest in some changes."

During the hearing, Target Chief Financial Officer John Mulligan reiterated that his company was "deeply sorry" for the data breach of its consumers' information.

"We are asking hard questions about whether we could have taken different actions before the breach was discovered that would have resulted in different outcomes," Mulligan said in his testimony.

The National Retail Federation supports a national standard for companies to notify customers, but is wary of legislation that would create "over-notification" standards that could desensitize the public from the most significant threats, David French, the trade group's senior vice president for government relations, has said.