Relating to economics, we can explore market failure theory. This breach highlights a failure in the provider's security systems, representing a market failure where private entities do not adequately manage risks, leading to external costs borne by customers (things like identity theft or financial loss). Secondly, there is the information asymmetry theory, where due to delayed law enforcement investigations, initial response, and platform provider delays lead to delayed notification of the breach, creating information asymmetry. Customers lack real-time awareness of the risks posed to their data. This can prevent customers from making timely, informed decisions to mitigate harm.

Trust between a company and its customers is critical when maintaining a positive business relationship. The tone of the letter and recommended actions, such as contacting law enforcement, signal an aim to rebuild trust that the data breach may have eroded. This theory of trust explores how breaches impact social and enterprise trust dynamics. Finally, the risk society theory associated with Ulrich Beck examines how modern societies manage and communicate risks, particularly technological ones. The breach demonstrates vulnerabilities inherent in digital transactions. It highlights the societal shift toward addressing pervasive risks in a connected economy, including strategies such as implementing better cybersecurity practices and providing consumer protection resources.