Two Economics Theories are cost-benefit analysis and information asymmetry. A cost benefit analysis theory is a central topic to the company’s cybersecurity decisions. The delayed discovery and response suggest that, historically, the platform provider may have underestimated the costs of a potential data breach versus the investment in more robust cybersecurity measures. The information asymmetry theory highlights how the letter had a classic case of information asymmetry. Where the company and its platform provider know more than the other. Customers were unaware of the breach for nearly a year, and the notification delay only heightened that imbalance.

Two Social Science Theories are trust and risk society. Trust between institutions and individuals is key in social systems. This letter is an attempt to restore trust after it was damaged. How the company manages communication, and transparency will influence how trust is either repaired or permanently broken. The risk society theory represents that modern societies are increasingly organized around managing risks. The data breach letter reflects how digital risks are now a normal part of corporate and consumer life.