**Economics Theories:**

1. **Information Asymmetry:** This theory is all about one party having more or better information than the other. In the case of this data breach, the company and its platform provider knew about the security issue way before the customers did. They were informed in February 2017, but the breach had been happening since February 2016. This delay in communication creates an imbalance—customers were using the site without knowing their data was at risk, which means they couldn't make informed decisions. That’s classic information asymmetry.
2. **Externalities:** This theory refers to the side effects of an economic activity that affect others who didn’t choose to be involved. Here, the company’s poor cybersecurity (or their platform provider’s, technically) caused a negative externality—customers now have to deal with the consequences, like replacing cards and watching for fraud, even though they didn’t cause the problem. The costs of the breach are being pushed onto the customers, not just the company.

**Psychological/Social Science Theories:**

1. **Trust Theory (Social Psychology):** Trust is a big factor in online shopping. People assume that companies are protecting their information. When something like this happens, it breaks that trust. Once trust is broken, it’s hard to earn back, especially if customers feel like the company didn’t act fast or transparently. That’s probably why this letter is trying so hard to reassure people that they’re “monitoring the platform” and “working with cybersecurity firms.”
2. **Cognitive Dissonance Theory:** This theory explains the discomfort people feel when their actions and beliefs don’t align. In this case, customers believed they were shopping safely, but now they find out their data may have been compromised for months. That’s a huge disconnect. The letter tries to reduce that discomfort by saying things like “we are unaware of any actual misuse” and by giving steps to take, which can make customers feel like they’re regaining some control.