**Week 12 – Journal Entry 12**

**Sheldon Horrell**

**CYSE-201S**

**4/6/25**

In reading this data breach notification from GlassWasherParts.com. It explains how malware had infected one of their provider’s systems, exposing customer payment data for almost a year. Customers weren’t told until months after it was discovered, because law enforcement asked them to wait to complete and investigation.

It is an economic and social problem we’re all facing. Economically, it shows how delayed transparency comes into play. In Verizon’s *Data Breach Investigations Report* (2023), which details out how long it often takes organizations to detect and disclose attacks, similar to the almost year long wait disclosed in this letter. Customers are left in the middle; often stuck with the costs they didn’t create.

From a Social science perspective, the breach creates distrust. Consumers expect companies to protect their information, not put them in the position of managing stolen data, canceling cards, and being on the lookout for future financial loss.

What’s most alarming is how common this has become that it’s a standardized and formatted letter/pdf you can just edit. Information systems breaches are becoming routine now, but we cannot just accept it. Every time it just chips away at the trust we place in sharing sensitive information over the internet. Personally, it’s reasons like this I have a second “Spending” account and debit card for online purchases, separate of my primary account. A simple form of protection from events just like this and takes just a few clicks to move the money.

**Reference**

Verizon. (2023). *Data Breach Investigations Report*. https://www.verizon.com/about/news/2023-data-breach-investigations-report?msockid=025ed661a170651b06a1c5c8a0f66474

Module 11 PowerPoint

Module 10 PowerPoint