Shanthan Kumar Bine - 991447982

Case Study 13.1

1. **As of this writing, there have been no fines levied against Equifax. Given that Equifax could legitimately claim that they are a victim here, does a fine appear to be warranted? Why or why not?**

A. Equifax's data breach has caused a massive exposure of sensitive information of over 147 million people, which lead to identity theft and other frauds. While Equifax's may claim as victim here but it is Equifax's failure to upgrade the infrastructure and patch the flaw that allowed hackers to access client data demonstrates a disregard for sensitive information security. Equifax is accountable, it is the company's duty to protect its client's personal information. I think Imposing huge fine's on business may be essential to promote moral conduct and guarantee responsibility while also avoiding further violations.

2. **What other laws do you believe should be passed? Would they have been helpful to prevent this breach?**

A. It may be possible to stop additional breaches by enacting laws requiring the disclosure of data breaches and penalizing companies that don't protect customer information. Laws requiring organizations to implement robust security controls and frequently upgrade their systems may also be advantageous.

3. **Given that over half of the adult U.S. population is vulnerable to identity theft from this breach alone, not to mention the other breaches described in Chapter 7, it is likely that your information makes you vulnerable to identity theft. If you live in the United States, what actions have you taken as a result of the breach?**

A. Residents of the United States can take preventative measures to safeguard themselves against identity theft. They should also regularly check their credit reports, freeze their credit reports, make strong, distinctive passwords, and exercise caution when disclosing personal information online.

4. **Please answer the same question about the usefulness of social security numbers. If they appear not to be useful any longer, what should the government do about this?**

A. Data breaches have reduced the value of social security numbers as a means of identifying people and granting access to financial services. To better protect the private information of citizens, the government must look into alternative forms of identity, like biometric authentication.

5. **What are the forces that would lead you to delay disclosing the breach to the public? Which of the issues are defensible? Which are not? Why?**

A. Organizations may be reluctant to disclose a breach due to worries about possible harm to their reputation, legal repercussions, and loss of business. However, delaying a breach notification can increase customer harm and make it more difficult for them to take the necessary precautions. Delaying disclosure is therefore not justifiable due to the possibility of further harm to people and harm to the company's reputation.

6. **Does the poor public relations fallout from the breach likely endanger the long-term success of Equifax? Why or why not?**

A. Customers might doubt Equifax's ability to protect their personal data as a result of the negative publicity the hack has generated. This could jeopardize the company's future success. Thus, there is a chance that this will cause a decline in business, harm to the industry, and harm to the reputation of the company. Though the effects might not be as severe as initially believed, Equifax's ability to recover and keep its federal contracts offers some hope.