How do the PCI DSS standards differ from general expectations of data security under Section 5 of the FTC Act and state data security laws?

The PCI DSS standard is the de facto information security standard for organizations that accept, use, process and store credit or debit card information. However, the standards are not adopted by courts or legislatures. Instead, it is adopted by an organization comprised of the major credit card companies which include Visa, MasterCard, American Express, and so on. The standard also includes detailed technical guidelines for organizations of any size that accept or use credit debit cards to comply with the PCI DSS requirements (Kosseff, 2017). When compared to the FTC section 5 act and other data security laws, the specific nature of PCI DSS and its goals and requirements make it different in its expectation of data security

Section 5 of the FTC Act gives the agency more power to enforce actions on companies that fail to comply with the PCI DSS requirements. The reason behind it is that PCI DSS audits are required by the major payment card issuing companies of retailers and other businesses that process more than 1 million card transactions in a given year. Additionally, the audits are intended to ensure that companies are providing adequate protection to consumers’ sensitive personal information (FTC, 2016). Hence, compliance with the prevailing standard seems to be an indicator of reasonable data security for the FTC.

On the other hand, when we look at state data security laws, states haven’t incorporated PCI DSS. However, the standard could help determine the general standard of care in common law tort and contract claims. Nevertheless, two state laws refer to PCI DSS. That is, the state of Nevada requires merchants to comply with the standards. However, Washington state requires businesses to “take reasonable care to guard against unauthorized access” to payment card information and exempts those who are certified for compliance with the standard from liabilities (Kosseff, 2017).

References

FTC. (2016). FTC To Study Credit Card Industry Data Security Auditing. Retrieved from https://www.ftc.gov/news-events/press-releases/2016/03/ftc-study-credit-card-industry-data-security-auditing

Kosseff, J. (2017). Cybersecurity Law. Hoboken, N.J: John Wiley & Sons, Inc.