Sprint 4: Coppa NY Shield Act

1. What is the law or regulation? (in simple terms)
    a. Children's Online Privacy Protection Act (COPPA) is a law that requires the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The primary goal of COPPA is to place parents in control over what information is collected from their young children (under 13) online. The information could be collected from operators of commercial websites and online services as well as general audience websites. (Vedova, 2023)
2. Why is it applicable to TKH?
    a. TKH is a nonprofit so it's under the category of those not subjected to COPPA but it would be encouraged to post privacy policies online and protect COPPA's protections to potential child visitors. TKH's website is not directed towards children under 13, both fellowships offered require students to be older than 13 so they would also not be knowingly collecting, using or disclosing personal information from children within that age group.
3. Does TKH's current secure program satisfy this legal or regulatory requirement? Yes or No and Why?
    a. TKH is technically not subjected to COPPA but it does have privacy policies when the user initially opens the page, therefore it does satisfy the legal requirement
4. What are the fines for violating this law or regulation?
    a. A court can hold operators who violate the Rule liable for civil penalties of up to $50.120 per violation. COPPA gives states and certain federal agencies authority to enforce compliance with respect to entities over which they have jurisdiction ("History of COPPA Violations", n.d.)

https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions

https://www.privo.com/history-of-coppa-violations#:~:text=The%20FTC%20enforces%20COPPA%20violations,over%20which%20they%20have%20jurisdiction.

A. What is the law or regulation? (in simple terms)

    a. Stop Hacks and Improve Electronic Data Security (SHIELD Act) is a law in New York that strengthens their data security laws by: (1) expanding the types of private information for which companies must provide customer notice in event of a breach and (2) requiring that companies develop, implement, maintain reasonable safeguards to protect the security, confidentiality, and integrity of the private information (“SHIELD Act”, n.d.)

B. Why is it applicable to TKH?
    a. TKH’s main office is house in New York (the Bronx specifically) so they must abide by this act

C. Does TKH’s current secure program satisfy this legal or regulatory requirement? Yes or No and Why?
    a. Without completing a penetration assessment we cannot for sure say if TKH’s current secure program satisfies this legal requirement *

D. What are the fines for violating this law or regulation?
    a. For failure to provide timely notification, the court may impose a civil penalty of up to $20 per instance of failed notification, not to exceed $250,000. For failure to maintain reasonable safeguards, the court may impose a civil penalty of up to $5,000 per violation (“SHIELD Act”, n.d.)

https://ag.ny.gov/resources/organizations/data-breach-reporting/shield-act#:~:text=Under%20the%20SHIELD%20Act%2C%20the,notification%2C%20not%20to%20exceed%20%24250%2C000.

References:

Fenton, H. (2018). Data Breaches: Nonprofits Are Also at Risk. Venable LLP. Retrieved from https://www.venable.com/insights/publications/2018/10/data-breaches-nonprofits-are-also-at-risk

Gibson, J. (2018). The Consequences of PCI DSS Non-Compliance. Tripwire. Retrieved from https://www.tripwire.com/state-of-security/regulatory-compliance/pci/consequences-of-pci-dss-non-compliance/

National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

New York State. (2020). Stop Hacks and Improve Electronic Data Security Act (SHIELD Act). https://www.nysenate.gov/legislation/laws/GBS/899-AA

United States Congress. (2002). Federal Information Security Management Act of 2002. https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf

PCI Security Standards Council. (2021). PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1. Retrieved from https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv321.pdf