GOVERNMENT AND REGULATORY AFFAIRS BLAST

US SAFE WEB Act of 2006

March 2015

AUTHOR

Blake Lovvorn, Insurance Coordinator for University of Central Florida and URMIA member.

STATUTE/REGULATION SOURCE

Federal Trade Commission Act of 1914 (the "FTC Act"), as amended by the Undertaking Spam, Spyware, And Fraud Enforcement With Enforcers beyond Borders Act of 2006 (the "U.S. SAFE WEB Act"), 15 U.S.C. § 41-58.

BRIEF DESCRIPTION

This briefing describes the Federal Trade Commission's foray into cyber security regulation using the existing Federal Trade Commission Act and the impact that can have on universities.

POTENTIAL/ACTUAL IMPACT

The Federal Trade Commission Act created and established the Federal Trade Commission (FTC) to prevent unfair or deceptive acts or practices in or affecting commerce through regulations, as well as monetary redress for conduct injurious to consumers. The FTC Act was further amended by the U.S. SAFE WEB Act to give the Federal Trade Commission tools to improve enforcement regarding privacy and security breaches among other consumer protection matters. The Federal Trade Commission has brought law enforcement actions against a variety of entities across a broad spectrum of industries who have failed to implement reasonable and appropriate security measures to protect consumer data[1]. Since 2002, the Federal Trade Commission has brought over 50 cases against entities specifically for data security failures[2]. The most recent case was against Wyndham Worldwide Corporation and three of its subsidiaries[3] in which the court affirmed the Federal Trade Commission's authority to challenge entities for unfair data security practices using 15 U.S.C. § 45. Wyndham has appealed the case to the Third Circuit Court of Appeals which will hear arguments in mid-March over the authority of the FTC to require companies to adopt data-security measures, so this is still an ongoing legal battle with precedent-setting potential.

The Wyndham case shows the Federal Trade Commission's continued move towards those entities whom it feels are not providing reasonable and appropriate security measures. To date, the FTC has not cited any universities for violating 15 U.S.C. § 45 for data security, but have cited a university's physician network for alleged price-fixing[5]. The increasing number of data breaches have pushed public support towards punishing those offenders which could include universities. Successful suits against universities for data security failures may have a significant reputational and financial impact.

DISCUSSION

The challenge for universities and others in higher education is the FTC's determination of "reasonableness." In this court case, FTC v. Wyndham Worldwide Corporation, the FTC argued that reasonableness can be evaluated by: (1) The data security measures of others in the same industry, i.e. higher education; (2) the FTC's business guidance brochure[4] and; (3) consent orders from previous FTC enforcement actions

In 2014, the SANS Institute published a white paper titled, "Higher Education: Open and

US SAFE WEB Act of 2006

Secure?[6]", which surveyed the higher education industry regarding their current cyber security practices. Some key findings from the report included: organizations lack of risk assessment policies, concerns with sensitive systems and data, lack of encryption, unclassified and unmanaged data, and under-staffed and under-funded departments managing cyber security. This report highlighted the many vulnerabilities of the industry, but also showed the similarities in data security measures taken by those organizations in the higher education sector, which is one criterion the FTC uses to evaluate "reasonableness".

The FTC's business guidance brochure titled, "Protecting Personal Information: A Guide for Business", lists 5 key principles on which a sound data security plan is built: (1) take stock; (2) scale down; (3) lock it; (4) pitch it; (5) plan ahead.

Understanding your individual systems and the data on them is the first step in identifying areas which require data security measures. The second principle, "scale down", may not apply to the higher education industry as the FTC recommends only keeping information that is needed and many universities, especially public universities, are subject to statutes which require keeping records for a number of years, so scaling down records may not be feasible. However, a useful tip from this principle is limiting information to only those employees who need access, especially Personally Identifiable Information (PII), Personal Health Information (PHI) and Family Educational Rights and Privacy Act (FERPA) data. Under the "lock it" principle, the FTC recommends ways to physically and electronically protect data, but on a large scale with such tools as firewalls, passwords, and locked storage. "Pitch it" identifies ways in which expired data should be properly disposed, this can be done through a third-party provider or simply ensure employee turnover security cards when leaving employment at the institution. Finally, "plan ahead" looks at ways of managing a cyber breach or incident, much like a Continuing Operations Plan (COOP), which should involve information technology, risk management, human resources, compliance, public relations and other offices your organization may want to include.

Recent FTC enforcement actions include requiring the establishment, implementation and maintenance of a comprehensive privacy program with at least an annual independent third-party professional audit and assessment. Additional actions include maintaining records and furnishing those records upon request to the FTC for a period of 5 years, written notice of any changes to the organization that may affect compliance under the enforcement actions, and agreement that the organization will not misrepresent the way the organization maintains and protects the privacy, security, confidentiality, or integrity of any covered information.

EXAMPLE

The US SAFE WEB Act amended the original FTC Act by adding additional sections and expanding some of their powers. The main benefit was adding language which allows the FTC to collaborate with foreign agencies. Although there may be examples of where the FTC has collaborated with foreign agencies, this report is limited to the FTC's use of existing laws (FTC Act and US SAFE WEB Act) to begin exerting authority over cyber security regulations.

ACTION

Organizations should review their current security and privacy program with their information security officer or equivalent individual in their organization. A third-party independent audit would allow for organizations to identify potential gaps in security which could result in an assessment by the FTC if not resolved. Additionally, there are multiple cyber security insurance policies on the market to help

organizations transfer some of the risk of a cyber-breach as well as provide coverage and assistance during a breach. This is a growing field in the insurance industry with multiple tools for organizations to assist with protecting their sensitive information prior to an incident.

SOURCES AND REFERENCES

1. "FTC Comment Before the FCC Concerning Proposed Cyber Security Certification Program," Federal Trade Commission (http://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-comment-fcc-concerning-proposed-cyber-security-certification-program/101013fcccomment.pdf)

2. "Federal Trade Commission 2014 Privacy and Data Security Update," Federal Trade Commission (http://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf)

3. Federal Trade Commission v. Wyndham Worldwide Corp., 10 F.Supp.3d 602 (D.N.J. 2014) (http://www.ftc.gov/system/files/documents/cases/140407wyndhamopinion.pdf)

4. "Protecting Personal Information, A Guide for Business," Federal Trade Commission (http://www.ftc.gov/system/files/documents/plain-language/bus69-protecting-personal-information-guide-business_0.pdf)

5. "Decision and Order: Washington University Physician Network," Federal Trade Commission (http://www.ftc.gov/sites/default/files/documents/cases/2003/09/wupndo.pdf)

6. "Higher Education: Open and Secure?," the SANS Institute (http://www.sans.org/reading-room/whitepapers/analyst/higher-education-open-secure-35240)

URMIA's Government and Regulatory Affairs Committee (GRAC) works to inform and educate URMIA's members about federal legislation and regulations. If you would like to become a member, have suggestions for future GRA Blasts, or have any questions, please contact URMIA at urmia@urmia.org.