The Cybersecurity Deficiencies That Create Liability: What You Must Know And Should Do

Educational Webinar with Fred Taylor and Sai Huda

Wednesday, July 8, 2020 | 2 pm PDT

Webinar Speakers

Frederick K. Taylor

Partner and Privacy & Cybersecurity Practice Group Co-Leader @Procopio

Sai Huda

Risk & Cybersecurity Expert, Author of the best-seller, Next Level Cybersecurity: Detect The Signals, Stop The Hack

Questions We Will Answer In This Webinar

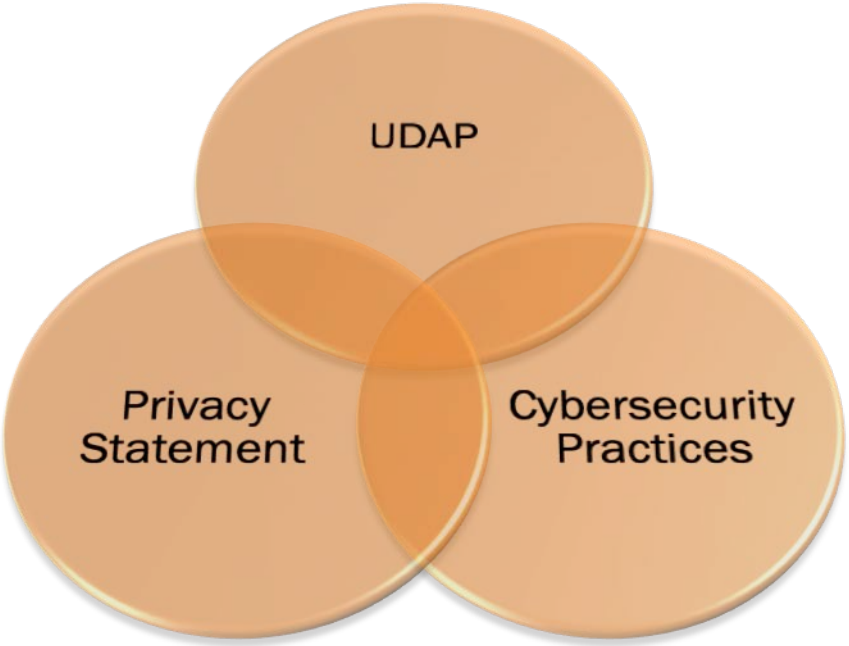
- Which cybersecurity deficiencies and practices create liability under federal and state unfair or deceptive acts or practices (UDAP) laws?
- How did cybersecurity deficiencies create a five year, thousands of dollars in UDAP liability even though there was no data breach or theft?
- How did cybersecurity deficiencies create over $700M in UDAP liability?
- How are regulators ramping up enforcement actions for privacy and cybersecurity deficiencies?
- What are the five critical steps and tools to mitigate cybersecurity deficiencies and UDAP liability before any damage is done?

UDAP Risk

Section 5(a) of the FTC Act provides that "unfair or deceptive acts or practices in or affecting commerce . . . are . . . declared unlawful." 15 U.S.C. Sec. 45(a)(1).

- Unfair acts or practices
  - if it causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.
- Deceptive acts or practices
  - If it involves a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances.

Cybersecurity Deficiencies Linkage To UDAP



Polling Question #1

Privacy Statement Failure Case

- CFPB charged that representations were false, because the company did not implement reasonable data-security practices even though it stated in privacy statement:
  - "All information is securely encrypted and stored"
  - "100% of your info is encrypted and stored securely"
  - "…encrypts all sensitive information that exists on its servers"
  - "…uses industry standard encryption technology"
  - "…encrypt[s] data in transit and at rest"
  - "…website, mobile applications, connection to financial institutions, back end, and even APIs use the latest encryption and secure connections"

Privacy Statement Failure Case

CFPB charged “Respondent’s representations regarding its data-security practices…were likely to mislead a reasonable consumer into believing that…had incorporated **reasonable** and appropriate data-security practices when it had not.” “Thus …. practices, as described in…. constitute **deceptive acts or practices.**”

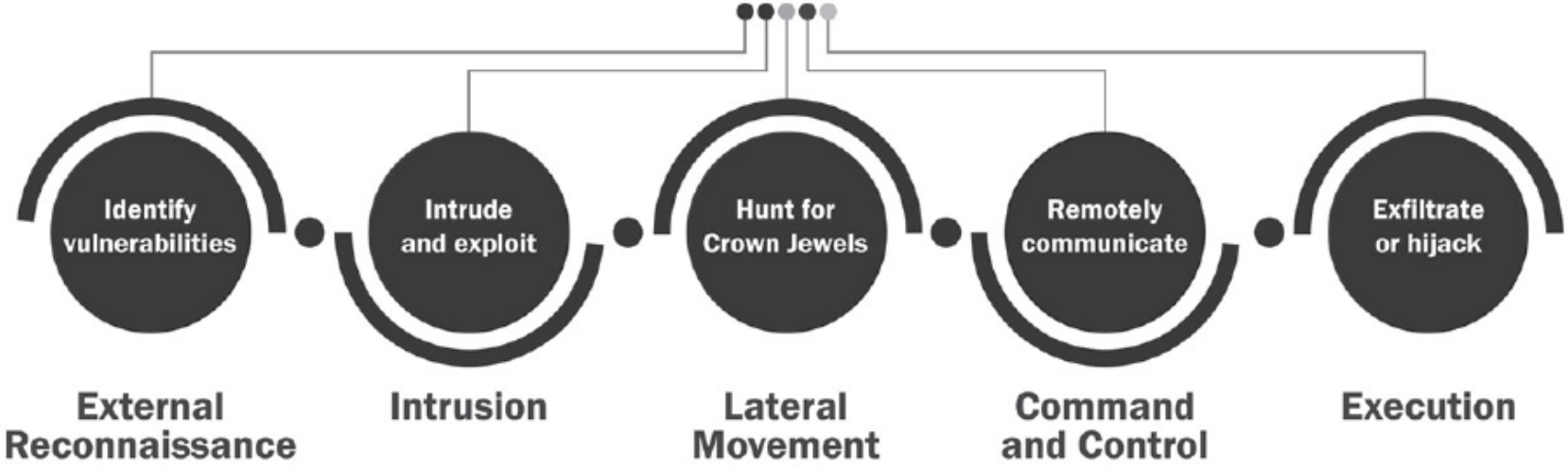
CFPB mandated:

- Consent Oder, $100,000 civil money penalty
- Enhanced Board oversight and compliance plan
- Implement Board approved “reasonable” data-security
- Twice a year data-security risk assessment
- Training of all employees on data-security
- Annual third party data-security audit
- Reporting of compliance progress to CFPB
- Five years notification of Consent Order requirements to new employees and suppliers
- Five years record-keeping of compliance with Consent Order

Cybersecurity Failure Case

- FTC charged cybersecurity deficiencies were unfair or deceptive acts or practices.
- Company settled consolidated class action lawsuits with FTC for **$700M**.
- Company estimates total cost will be over **$1.3B**.
- FTC ramping up enforcement actions for cybersecurity deficiencies.
- Plaintiff Attorneys and States following FTC's lead with enhanced scrutiny.

Cyber Attack Chain



Source: Next Level Cybersecurity: Detect The Signals, Stop The Hack

Unfair Acts or Practices in $700M Case

- Critical and high-risk vulnerabilities were unpatched for months allowing hackers to exploit.
- Failing to maintain accurate inventory of public facing technology assets.
- Failing to segment servers and databases.
- Inadequate host and network intrusion detection or file integrity monitoring for unauthorized access to network.
- Failing to log or monitor privileged account activity.

Unfair Acts or Practices in $700M Case

- Storing administrative credentials in plain text.
- Sensitive personal information were accessible to employees and contractors without any business need.
- Failing to maintain security certificates to enable examining traffic for suspicious activity.
- Failing to implement protections against XSS, SQL injections.
- Failing to provide adequate security training to engineers and other employees.

Deceptive Acts or Practices in $700M Case

- The company's privacy statement represented:

  "We are committed to protecting the security of your information through procedures and technologies designed for this purpose by taking these steps: We limit access to your personal information to employees having a reasonable need to access this information to provide products and services to you . . . We have reasonable physical, technical, and procedural safeguards to help protect your personal information."

- The FTC charged the many security failures failed to provide "reasonable safeguards" over consumer data and violated the GLBA, and the representations in the privacy statement were false or misleading and constitute a deceptive act or practice.

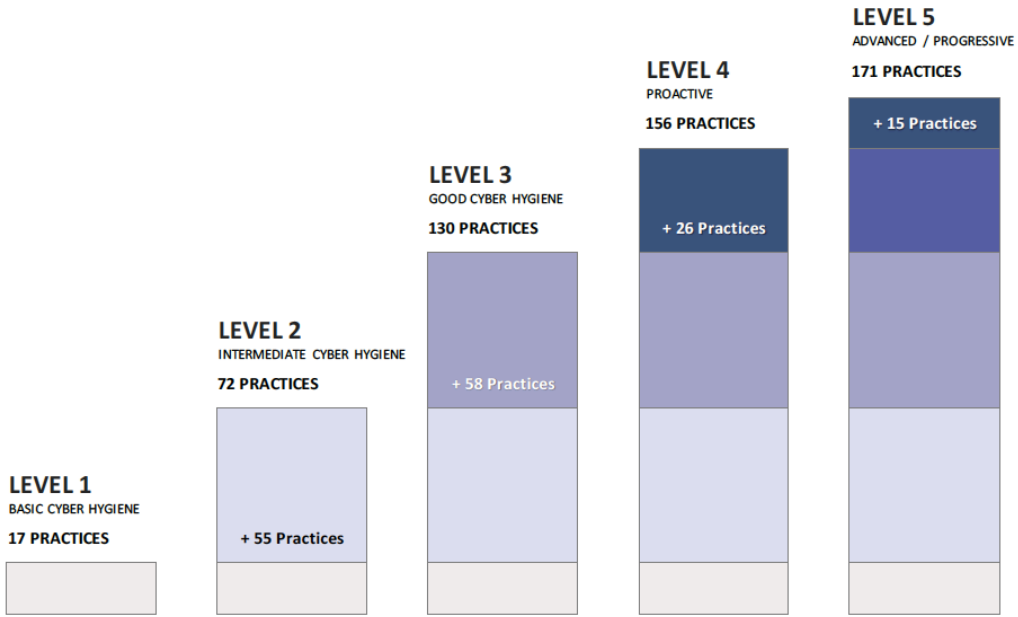
What is “Reasonable Security”?

- There is no legal definition.
- Subject to regulatory enforcement actions and class action lawsuit settlements.
- A helpful guide is **FTC’s “Start with Security: A Guide for Business”**
  - Outlines 10 cybersecurity best practices.
    - Start with security
    - Control access to data sensibly
    - Require secure passwords and authentication
    - Store sensitive PI securely
    - Segment your network and monitor it
    - Secure remote access to your network
    - Sound security when developing new products
    - Make service providers use reasonable security measures
    - Procedures for security and new vulnerabilities
    - Secure paper, physical media, and devices
  - Good source for what FTC deems to be **“reasonable security.”**

Polling Question #2

NIST 800-171r1 and CMMC

- Other sources for **“reasonable security”** are:
  - NIST 800-171r1 and 110 cybersecurity practices
  - Cybersecurity Maturity Model Certification (CMMC) for defense contractors
    - Mandatory cybersecurity practices
    - Level 1 – 5 certification by third party auditor



Source: CMMC, Version 1.0, January 2020, DoD

Five Key Risk Mitigation Action Steps

1. Provide UDAP Briefing and Training to Board and Management
2. Conduct UDAP Risk Assessment
3. Perform Privacy Statement Audit
4. Implement NIST 800-171r1 110 Cybersecurity Practices
5. Implement FTC's "Reasonable Security" Best Practices

Thank You and Q&A

For UDAP Risk Assessment, Privacy Statement Audit or UDAP Briefing or Training, contact:

- Fred Taylor, Partner and Privacy & Cybersecurity Practice Group Leader
- Fred.Taylor@procopio.com
- 619-515-3279