Ballard Spahr LLP

Privacy and Data Security Developments

Pennsylvania Bar Institute

Consumer Financial Services & Banking Law Update

Kim Phan
Partner, Privacy & Data Security Group
Ballard Spahr LLP
(202) 661-7647
phank@ballardspahr.com

Ballard Spahr LLP

Agenda

- Privacy
- Data Security
- Breaches

2 |

Ballard Spahr LLP

Ballard Spahr LLP

California Consumer Privacy Act

Ballard Spahr LLP

Key Dates

- **June 28, 2018**: CCPA signed into law.
- **October 2019**: California Attorney General issued proposed regulations. Public hearings are scheduled on December 2nd, 3rd, 4th, and 5th. Public comments due by December 6, 2019.
- **January 1, 2020**: CCPA effective date.
- **Earlier of July 1, 2020 or 6 months after the implementing regulations are issued**: CCPA enforcement date.

4 |

Ballard Spahr LLP

CCPA Applicability

- The CCPA applies to any business, including any for-profit entity that collects consumers' personal data, which does business in California, and satisfies at least one of the following thresholds:
  - Has annual gross revenues in excess of $25 million;
  - Possesses personal information of 50,000+ consumers, households, or devices; or
  - Earns more than half of its annual revenue from selling consumers' personal information.
- Some exemptions may apply:
  - Personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act.
  - Consumer report information if use of the information is limited by the federal Fair Credit Reporting Act.
  - Personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act.
  - Protected health information collected by covered entities under the Health Insurance Portability and Accountability Act.

Ballard Spahr LLP

CCPA Requirements

- Enhanced disclosures, including in online privacy policies and when personal information is collected.
- Consumer rights, including information access, the right to be forgotten, the right to opt out of certain third party information sharing, and the right to equal service regardless of exercising any privacy rights.
- Reasonable security procedures and practices appropriate to the nature of the information.
- Violations of these requirements could result in:
  - Civil penalties in the amount of $7,500 for each intentional violation and $2,500 for each unintentional violation; and
  - If the violation involves a data breach, a private right of action conferring statutory penalties between $100 to $750 per California resident and incident, or actual damages, whichever is greater.

Ballard Spahr LLP

Ballard Spahr LLP

FTC GLBA Safeguards Rule Updates

Ballard Spahr LLP

Information Security Program Requirements

Current Requirements

- Administrative, technical, and physical safeguards
- Appropriate for the size and complexity of the financial institution, the nature and scope of the financial activities, and the sensitivity of information
- Reasonably designed to ensure security and confidentiality of information
- Protect against anticipated threats or hazards

Ballard Spahr LLP

Information Security Program Requirements

New Requirements

- Chief Information Security Officer (CISO)
- Risk assessments
- Access controls
- Data inventory
- Encryption
- Secure application development
- Multi-factor authentication
- Audit trails
- Secure disposal
- Change management
- Monitoring
- Information security personnel
- Training
- Service provider oversight
- Incident response plan

Ballard Spahr LLP

FTC Rulemaking Process

- **August 2016**: FTC solicited comments on the Safeguards Rule as part of a periodic review of its regulations.
- **April 2019**: FTC published its notice of proposed rulemaking.
  - Based primarily on NYDFS Cybersecurity Regulations and National Association of Insurance Commissioners data security model law.
- **TBD**: FTC publication of final rule.

- <u>FTC Commissioner Dissent – Primary Criticisms</u>
  - Overly prescriptive despite continuously evolving standards
  - No evidence of reducing data security risks or significantly increasing consumer benefits
  - Lack of flexibility handicaps small players and new entrants
  - Based on recent NYDFS regulations without data on the impact and efficacy of those regulations

Ballard Spahr LLP

Ballard Spahr LLP

The Capital One Data Breach

Ballard Spahr LLP

Capital One Breach

- 106 million account holders or applicants.
- Estimated cost in 2019 alone = $150 million.
- An unnamed, white hat "external security researcher" emailed Capital One on July 17th about customer data being stored in a publicly accessible file on GitHub. (127 days after hack began)
- Hacker = former employee of Amazon Web Services.
  - Scanned the Internet for vulnerable computers.
  - Identified a Capital One computer that manages communications between the company's cloud and the public Internet had a firewall misconfiguration.
  - Tapped into Amazon's metadata service to obtain credentials to access cloud servers of Capital One and up to 30 other companies.

Ballard Spahr LLP

Cloud Management Program

- Board level involvement
- Due diligence
- Contractual protections
- Written policies and procedures
- Training
- Monitoring and auditing
- Business continuity planning

CONSIDERATIONS
Governance
Compliance
Oversight
Architecture
Identity and Access Mgmt.
Data + Software Isolation
Data Protection
Confidentiality
Availability
Integrity
Security
Incident Response
Etc.

Ballard Spahr LLP

Resources – Recent Guidance

- FFIEC Press Release Encouraging Standardized Approach to Assessing Cybersecurity Preparedness (August 2019)
- FinCEN Advisory to Financial Institutions on E-mail Compromise Fraud Schemes (July 2019)
- FTC Data Breach Response: A Guide for Business (May 2019)
- FFIEC Cybersecurity Resource Guide for Financial Institutions (October 2018)
- DOJ Best Practices for Victim Response and Reporting of Cyber Incidents (September 2018)
- Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs (April 2018)

Ballard Spahr LLP

Ballard Spahr LLP

Thank You!

Ballard Spahr LLP