PROGRAM MATERIALS
Program #30203
September 1, 2020

What's Reasonable? Recent Developments in Cybersecurity Law

Celesq® AttorneysEd Center
www.celesq.com

5255 North Federal Highway, Suite 310, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Arent Fox

What's Reasonable?: Recent Developments in U.S. Cybersecurity Law

September 1, 2020, 12:00 P.M. Eastern Time

Presented by:
Julia B. Jacobson, Partner, and Natalia J. Kerr, Attorney
Arent Fox LLP (Boston)

Arent Fox

AGENDA

1. Introduction
2. The Legal Landscape
3. Assessing Reasonableness

Appendix: Sources

Arent Fox

Introduction

Arent Fox

Data Security Risk are on the Rise

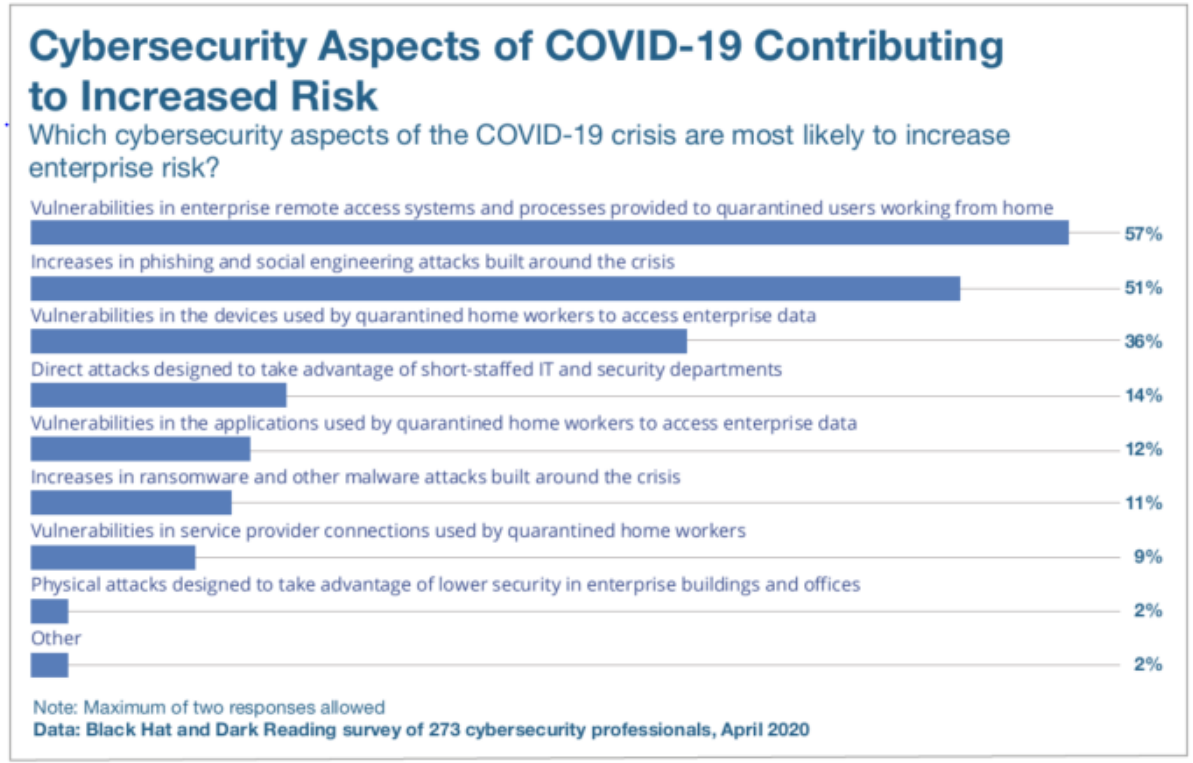
- **Average total cost of a data breach: 3.76 million USD and increases to $4M for an organization with a remote workforce**
  - Cost of a Data Breach Report 2020 (July 2020) https://www.ibm.com/security/data-breach (*Survey independently conducted by the Ponemon Institute and based on quantitative analysis of 524 recent breaches across 17 geographies and 17 industries*)

- **Hacking featured in 45% of surveyed breaches; errors were causal events in 22% of surveyed breaches with the top 3 error types as misconfiguration, misdelilvery and publishing errors**
  - Verizon 2020 Data Breach Investigations Report (May 21, 2020) https://www.verizon.com/about/news/media-resources/attachment?fid=5ec66f232cfac22c9a35796d

- **Average ransom payment increased by 33% to $111,605 from Q4 2019 to Q1 2020**
  - 2020 Ransomware Marketplace Report (April 29, 2020) https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report)

Arent Fox

Data Security Risk are on the Rise



https://i.blackhat.com/docs/usa/2020/P3_28203_BH20_Report.pdf

Last accessed August 25, 2020

Arent Fox

The Challenge

Data security laws in regulated industries are more prescriptive than general data security laws, rules and regulations.

The Challenge

General data security laws typically require “reasonable” and/or “appropriate” data security measures …

The Challenge

… because (in part) they are designed for flexibility to accommodate evolving business needs, resources, risk tolerance and technological advances.

Arent Fox

The Challenge

Businesses operating outside regulated industries must sift through a patchwork of laws, guidance and enforcement actions.

The Challenge

How do you counsel a business about whether a data security program is “reasonable”?

Arent Fox

View (in 2018) from the Bench

"In sum, assuming arguendo that LabMD's negligent failure to implement and maintain a reasonable data-security program constituted an unfair act or practice under Section 5(a) [of the FTC Act], the [FTC's] cease and desist order is nonetheless unenforceable. It does not enjoin a specific act or practice. Instead, it mandates a complete overhaul of LabMD's data-security program and says precious little about how this is to be accomplished. Moreover, it effectually charges the district court with managing the overhaul. This is a scheme Congress could not have envisioned."

LabMD, Inc. v. F.T.C., 894 F.3d 1221, 1229 (11th Cir. 2018), which vacates LabMD, Inc., Docket No. 9357 (F.T.C. July 28, 2016), https://www.ftc.gov/system/files/documents/cases/160729labmdorder.pdf

Today's Focus

Recent U.S. data security developments from the Federal Trade Commission (FTC) and various states that offer common data security requirements to help you guide a business in developing its data security program.

Arent Fox

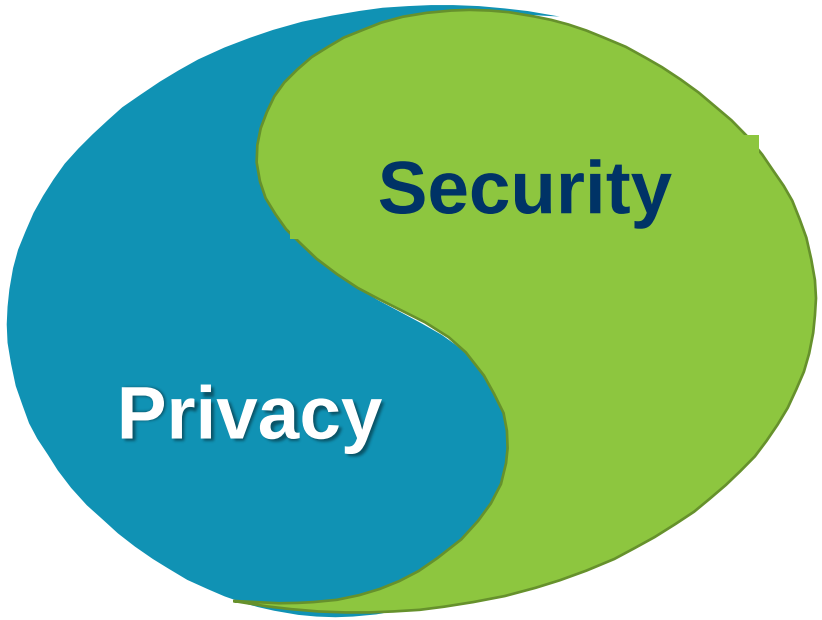
Data Security Basics

Arent Fox

Privacy vs. Security

"Right of Privacy"

- Fairness of Use
- Notice
- Choice
- Access
- Accountability
- Security



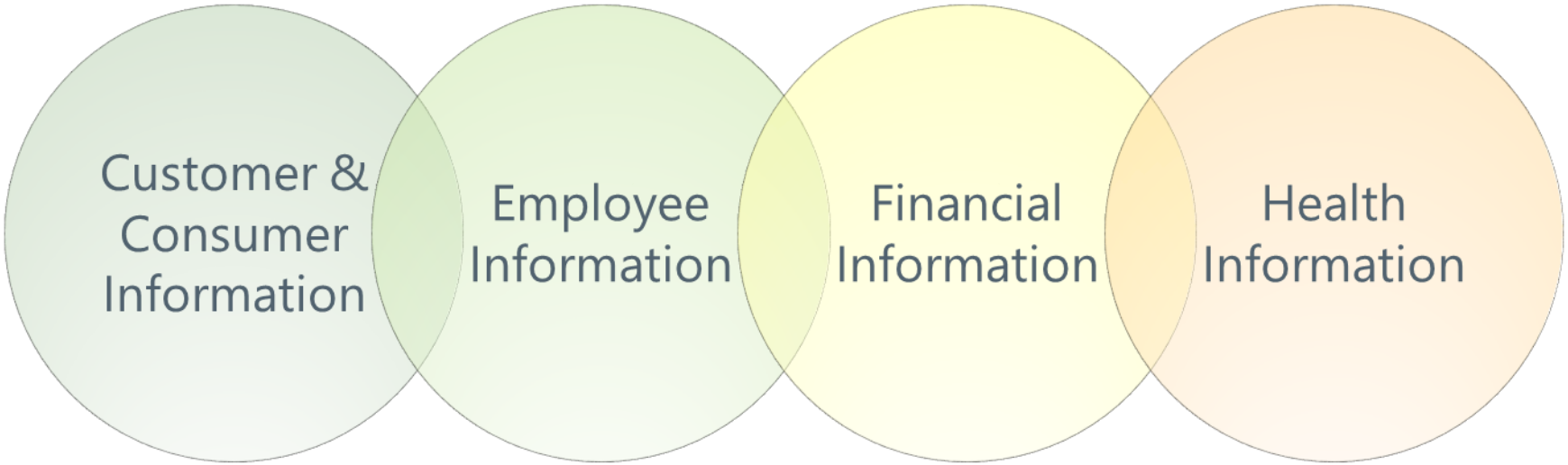
Security

- Availability
- Integrity/Quality
- Retention
- Storage/Backup
- Encryption
- Destruction

Arent Fox

Privacy Laws: What Do They Protect?

Personal information (aka personal data)



Data Security: What Does a Data Security Program Protect?

Protection for:

- **Personal information** – as defined under privacy laws
- **Confidential information**, which may include personal information – typically required to protect by contract
- **Trade secrets** – owner must reasonable measures to keep the information secret

Data Security: What Does a Data Security Program Protect?

Protection for privacy torts:

- **Right of Publicity** – public disclosure of private facts when facts disclosed are not a public concern
- **Right of Privacy** – private affairs become public and intrusion is highly offensive
- "**False light**" – public disclosure of false information

Arent Fox

Legal Landscape

Arent Fox

Primary Sources of U.S. Data Security Law

Industry-Specific Data Security Laws (state and federal)

- The U.S. generally follows the "sectoral approach" to data security (and privacy) regulation, i.e., more developed laws to economic sectors (*e.g.*, public, private, financial, online, offline); *cf.* omnibus approach, *i.e.*, a single comprehensive data protection law that applies to most sectors, like General Data Protection Regulation

Federal Trade Commission (FTC) Act and State "Mini FTC Acts" and Enforcement

State General Data Security Laws and Enforcement

- Approximately 22 states have laws that require "reasonable security" of which 15 do not provide details about what "reasonable security" entails (www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx; see Appendix)

Arent Fox

Industry-Specific Data Security Laws

Arent Fox

Data Security Laws

Examples of Industry-Specific Laws, Regulations and Rules (*U.S. federal*)

Gramm-Leach-Bliley Act's Safeguards Rule - requires financial institutions to develop, implement, and maintain reasonable administrative, technical, and physical safeguards "reasonably designed" to protect the security, confidentiality, and integrity of customer information.

- July 13, 2020: FTC Workshop on Proposed Changes to Safeguards Rule
  - Seeks to "maintain the flexibility" of the current Safeguards Rule and also "provid[e] more guidance about the contents of an information security program" while "still allowing the financial institution to create a program that is adapted to its particular needs"
  - Slides from Workshop - https://www.ftc.gov/system/files/documents/public_events/1567141/slides-glb-workshop.pdf (*last accessed August 27, 2020*)

Arent Fox

Data Security Laws

Examples of Industry-Specific Laws, Regulations and Rules (*U.S. federal*)

Health Insurance Portability and Accountability Act (HIPAA) Security Rule,
"The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce."

https://www.hhs.gov/hipaa/for-professionals/security/index.html (*last accessed August 27, 2020*)

Arent Fox

Data Security Laws

Examples of Industry-Specific Laws, Regulations and Rules (*U.S. state*)

- **Massachusetts Supreme Judicial Court Rule 1:24: Protection of personal identifying information in publicly accessible court documents**

  Subject to some limited exceptions, any person or entity that files documents in a Massachusetts state court must redact all personal information using the specified redaction methods. Similarly, the courts must "avoid" using personal identifying information in any court order, decision or court-issued document. For purposes of SJC Rule 1:24, "personal information" is defined as government issued identifiers (social security number, taxpayer identification number, driver's license number, state-issued identification card number or passport number), parents' birth surnames (when identified as such), financial account numbers and credit and debit card numbers.

  https://www.mass.gov/supreme-judicial-court-rules/supreme-judicial-court-rule-124-protection-of-personal-identifying (*last accessed August 27, 2020*)

Arent Fox

Data Security Laws

Examples of Industry-Specific Laws, Regulations and Rules (*U.S. state*)

South Carolina Insurance Data Security Act, S. C. Code Ann. § 38-99-10, https://www.scstatehouse.gov/code/t38c099.php

- **Section 38-99-20.** Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody, or control, each licensee shall develop, implement, and maintain a comprehensive written information security program based on the licensee's risk assessment and that contains administrative, technical, and physical safeguards for the protection of nonpublic information and the licensee's information system

Other states have passed or have pending insurance industry data security laws based generally on a 2017 model law by the National Association of Insurance Commissioners (e.g., Michigan, New Hampshire (see Appendix))

Arent Fox

Data Security Laws

Examples of Industry-Specific Laws and Regulations (*U.S. state*)

Vermont Securities Regulations (S-2016-01) § 7-8: Cybersecurity Procedures, https://dfr.vermont.gov/reg-bul-ord/vermont-securities-regulations

- A Vermont registered investment adviser must establish and maintain written policies and procedures reasonably designed to ensure cybersecurity … the cybersecurity policies and procedures must provide for: (1) An annual cybersecurity risk assessment; (2) The use of secure email, including use of encryption and digital signatures; (3) Authentication practices for employee access to electronic communications, databases, and media; (4) Procedures for authenticating client instructions received via electronic communication; and (5) Disclosure to clients of the risks of using electronic communications
- Vermont registered investment adviser must maintain evidence of adequate insurance for the risk of cybersecurity breach.

Arent Fox

Data Security Laws

Examples of Industry-Specific Regulations (*U.S. state*)

New York Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies (23 NYCRR 500)

https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

- Introduction: "… This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion. Senior management must take this issue seriously and be responsible for the organization's cybersecurity program and file an annual certification confirming compliance with these regulations."
- Effective 2017 with two-year transitional period for compliance

Arent Fox

NYDFS Cybersecurity Requirements

Detailed responsibilities on covered entities include:

- Written cybersecurity policy
- Qualified individual responsible for overseeing and implementing the cybersecurity program
- Periodic employee training
- Limitations on access privileges
- Monitoring activity of authorized users
- Multi-factor authentication
- Penetration testing and vulnerability assessments
- Application security
- Encryption
- Data minimization
- Vendor management

Regulated entities have 72 hours to notify the Superintendent of Financial Services about a Cybersecurity Event

Arent Fox

Enforcement of NYDFS Cybersecurity Requirements

July 21, 2020: first-ever NYDFS Statement of Charges alleges that First American Title Insurance Company exposed more than 850 million address documents containing consumers' sensitive personal information due to a known vulnerability on a public-facing website which made customer information "available to anyone with a web browser"… in the six months following discovery of the [vulnerability], [First American] failed to correct the vulnerability even though hundreds of millions of documents were exposed" because (inter alia) First American "failed to follow its own cybersecurity policies"; "failed to heed advice proffered by its own in-house cybersecurity experts"; and "remediation was ineffectively assigned to an unqualified employee".

https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202007221#:~:text=In%20the%20statement%20of%20charges,after%20it%20was%20discovered%20in

Arent Fox

Federal and State Data Security Laws and Enforcement

Arent Fox

Federal Trade Commission

Section 5 of the Federal Trade Commission Act of 1914 prohibits "unfair or deceptive acts or practices in or affecting commerce"

- **Unfair** - causes or is likely to cause substantial injury to consumers that they cannot reasonably avoid and that is not outweighed by countervailing benefits to consumers
- **Deceptive** - representation, omission or practice must mislead (or be likely to mislead) a consumer and is material

Arent Fox

Federal Trade Commission

Earliest enforcement in the FTC archives with a “Data Security” tag:

- For a deceptive act or practice*:* **FTC v. Sandra L. Rennert** (July 6, 2000)(*alleging that the defendants’ false representation “expressly or by implication, that the information customers provide to their Web sites is encrypted and that defendants use an SSL secure connection when transmitting this information over the Internet” constitutes a deceptive act or practice, in violation of Section 5(a) of the FTC Act*)
- For an unfair act or practice*:* **In re BJ’s Wholesale Club, Inc.** (Sept. 20, 2005)(*alleging that failure to employ reasonable and appropriate security measures was an unfair act or practice*)

Arent Fox

Federal Trade Commission

FTC Report to Congress - June 19, 2020

- "To date, the [FTC] has brought more than 70 cases alleging that companies failed to implement reasonable data security safeguards."
- "[in 2019], the [FTC] worked to strengthen data security orders to require board-level oversight of data security issues where appropriate, set forth more specific requirements (e.g., requirements to encrypt data, segment networks) …"
  - Footnote 15 *:* "The appellate court decision in LabMD also was part of the impetus for the Commission to re-evaluate the data security provisions in its orders. In that decision, the court found, inter alia, that the requirement to "establish, implement, and maintain a reasonable data security program" was "unenforceable because of lack of specificity."

See also January 6, 2020 FTC blog post touting significant improvements in its 2019 orders that involved data security issues: https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance.

Arent Fox

FTC Enforcement Actions – 2019-2020 (to date)

2019 and 2020 FTC Enforcement Actions include the same basic requirements as earlier enforcement actions but also elaborate.

Requirement	2019 and 2020 Enforcement Actions
Risk Assessment	• Conduct risk assessments at least once every 12 months and not later than 30 days following a data security–related event. (*See* i-Dressup)
Testing and Monitoring	• Test the security program at least once every 12 months and not later than 30 days following a data security–related event (*See* Tapplock) • Network vulnerability testing once every four months and not later than 30 days after a data security–related event (*See* Tapplock) • Network penetration testing at least once every 12 months and not later than 30 days after a data security–related event (*See* Tapplock) • Modify security program at least once every 12 months to reflect changes in the business' risk profile, operations and technology developments (*See* i-Dressup)

Arent Fox

FTC Enforcement Actions – 2019-2020 (to date)

Requirement	2019 and 2020 Enforcement Actions
Accountability	• Designate a "qualified" employee to oversee the security program (*See* Tapplock) • Require a written status report to the board and management "at least once every twelve months" and "promptly" after a data security–related event (*See* Tapplock)
Training	• Train employees at least once every 12 months (*See* Lightyear) • Provide biennial" security training for personnel and vendors responsible for developing software *(See* D-Link)
Vendor Management	• Only select vendors capable of safeguarding data • Contractually obligate vendors to maintain safeguards • Verify compliance (*See* Retina-X)

See Appendix for citations

Arent Fox

Massachusetts Data Security Law & Regulations

Massachusetts Data Security Law (Mass. Gen. Law Ch. 93H) is implemented by "Standards For The Protection Of Personal Information Of Residents Of The Commonwealth" (201 Mass. Code Regs. 17.00)

- Massachusetts was a leader among U.S. states when the data security law was enacted in 2007 (*n.b.,* data security regulations followed in 2010)

- Still among the most prescriptive general state data security laws

Arent Fox

Massachusetts Data Security Law & Regulations

- Applies to individual natural persons, legal entities and state government agencies that own or license certain personal information (*n.b.,* a relatively narrowly defined term) about Massachusetts residents

- Requirements are qualified by whether they are "**technically feasible**", which means reasonable means through technology to accomplish the required result

- The Massachusetts data security regulations have **ten general minimum requirements** for a written information security program (WISP) and **eight computer security** minimum requirements

Arent Fox

Massachusetts Data Security Law & Regulations

Ten general minimum requirements for a written information security program (WISP)

1. Designation of one or more employees responsible for the WISP
2. Assessments of risks to the security, confidentiality and/or integrity of personal information [a defined term] and the effectiveness of the current safeguards for limiting those risks, including ongoing employee and independent contractor training, compliance with the WISP and tools for detecting and preventing security system failures
3. Employee security policies relating to protection of personal information outside of business premises
4. Disciplinary measures for violations of the WISP and related policies
5. Access control measures that prevent terminated employees from accessing personal information

Arent Fox

Massachusetts Data Security Law & Regulations

Ten general minimum requirements for a WISP (*cont.*):

6. Management of service providers that access personal information as part of providing services directly to the person, including retaining service providers capable of protecting personal information consistent with the data security regulations and other applicable laws and requiring service providers by contract to implement and maintain appropriate measures to protect personal information
7. Physical access restrictions for records containing personal information and storage of those records in locked facilities, storage areas or containers
8. Regular monitoring of the WISP to ensure that it is preventing unauthorized access to or use of personal information and upgrading the WISP as necessary to limit risks
9. Review the WISP at least annually or more often if business practices that relate to the protection of personal information materially change
10. Documentation of responsive actions taken in connection with any “breach of security” and mandatory post-incident review of those actions to evaluate the need for changes to business practices relating to protection of personal information

Arent Fox

Massachusetts Data Security Law & Regulations

The eight **computer security** minimum requirements are:

1. Secure user authentication protocols including control of access credentials and reasonably secure methods for assigning, selecting, controlling and protecting passwords (such as use of biometrics or other unique identifier technologies); access control, including access for active users and accounts only, blocking access after multiple unsuccessful access attempts
2. Secure access control, including maintaining least-privilege/need-to-know access and assigning user ID plus passwords (not vendor supplied default passwords)
3. Encryption of personal information that travels across public network and transmitted wirelessly
4. Reasonable monitoring of systems for unauthorized use of or access to Personal Information

Arent Fox

Massachusetts Data Security Law & Regulations

The eight **computer security** minimum requirements are:

5. Encryption of personal information stored on laptops or other portable devices
6. Up-to-date firewall protection and operating system security patches
7. Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis
8. Education and training of employees on the proper use of the computer security system and the importance of personal information security

Arent Fox

Massachusetts Attorney General Settlement with Equifax

Equifax (*Commonwealth v. Equifax, Inc.*, No. 1784CV03009BLS2 (Mass. Super. March 31, 2020))

- Multi-state settlement resulting from cyber attack against Equifax (see, e.g., https://www.mass.gov/equifax-data-breach and https://www.equifaxbreachsettlement.com/)
- Personal information of approximately 147 million individuals was affected (three million are Massachusetts residents)
- Massachusetts Attorney General Healey settled with Equifax for "a record $18 million penalty" (https://www.mass.gov/service-details/ag-healeys-settlement-with-Equifax)

Arent Fox

Massachusetts Attorney General Settlement with Equifax

The Massachusetts Equifax Judgment requires that:

- Equifax hire “an executive or [security] officer” (**CISO**) responsible for implementing, maintaining and monitoring the data security program and ensure that he or she receives the necessary resources and support.
- Equifax’s CISO report to Equifax’s board and senior management annually and quarterly concerning the security posture or security risks and within 48 hours after discovery of any “compromise or threat that gives rise to a reasonable likelihood of compromise, by unauthorized access or inadvertent disclosure” of personal information of 500 or more U.S. residents
- Equifax hire security professionals with “the education, qualifications, and experience appropriate to the level, size, and complexity of her/his role” and train them prior to “starting their responsibilities” for the security program; design
- Equifax implement a written incident response plan and conduct, at a minimum, biannual incident response plan exercises to test and assess preparedness and require by contract that vendors provide notification within seventy-two hours of discovering a data security incident.

Arent Fox

Massachusetts Attorney General Settlement with Equifax

The Massachusetts Equifax Judgment requires that Equifax:

- Undertake response plan exercises to test and assess preparedness and require by contract that vendors provide notification within seventy-two hours of discovering a data security incident.
- Use automated tools to continuously monitor networks for active threats and assess the monitoring tools at least monthly;
- Complete at least one weekly vulnerability scan of all systems;
- Conduct remediation planning within twenty-four hours after discovery of a critical vulnerability and complete remediation within one week;
- Implement detailed access control that includes at least password strength, confidentiality and rotation requirements, two-factor authentication, encryption of administrative-level passwords, and user access inventory and termination procedures and secure storage of passwords based on industry best practices; network segmentation (e.g., disable unnecessary ports and logically separate production and non-production environments); process for managing and documenting changes to Equifax's network; manual processes and automated tools to inventory, classify and document all network assets ("software, applications, network components, databases, data stores, tools, technology, and systems"); digital certificates used to authenticate servers and systems that expire longer than one week after creation; and appointment of a "Patch Supervisor" to lead a "Patch Management Group."

Common Law Negligence Standard

The reasonable standard in various general data security laws may feel familiar to attorneys because of its similarity to the common-law negligence standard.

- For example: Portier v. NEO Tech. Sols (Case No. 3:17-cv-30111-TSH)(D. Mass. Dec. 31, 2019)
  - The decision of the U.S. District Court in this recent and on-going case found defendant NEO Technology Solutions ("**NEO Tech**") liable for negligence for failing to protect sensitive personal information of its employees.
    https://scholar.google.com/scholar_case?case=14377481689158676349&q=Portier+v.+NEO+Tech.+Sols,&hl=en&as_sdt=40000006&as_vis=1

Arent Fox

Portier v. NEO Tech. Sols

"Plaintiffs allege that NEO Tech breached its duty to exercise reasonable care in 'holding, safeguarding and protecting' the Plaintiffs' W-2 data from 'wrongful disclosure' by failing to 'maintain proper security measures, policies and procedures' and train its employees to guard against the unauthorized release of the data (Dkt. No. 45 ¶¶ 84, 88). Defendants counter that they complied with any duty they had by password protecting their W-2 data and by timely notifying employees of the breach (Dkt. No. 49 at 20) ... Because Plaintiffs claim that Defendants failed to employ reasonable security measures, including encryption, which was recommended by the Information Technology Department after two previous data breaches and to adequately train its employees to guard against a phishing scam, the Complaint adequately alleges that Defendants breached their duty of reasonable care."

*No. 3:17-CV-30111-TSH, 2019 WL 7946103, at *11-13 (D. Mass. Dec. 31, 2019), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020)*

Arent Fox

NY Shield Act

Stop Hacks and Improve Electronic Data (SHIELD) Act

- Effective March 21, 2020
- **Reasonable administrative safeguards**, such as (i) designating one or more employees to coordinate the security program; (ii) identifying reasonably foreseeable risks; (iii) assessing the sufficiency of safeguards to control the identified risks; (iv) training employees in security practices and procedures; (v) selecting service providers capable of maintaining appropriate safeguards, and requiring those safeguards by contract; and (vi) adjusting the security program to address business changes.

Arent Fox

NY Shield Act

- **Reasonable technical safeguards**, such as (i) assessing risks in network and software design; (ii) assessing risks in information processing, transmission and storage; (iii) detecting, preventing and responding to attacks or system failures; and (iv) regularly testing and monitoring the effectiveness of key controls, systems and procedures.
- **Reasonable physical safeguards**, such as (i) assessing risks of information storage and disposal; (ii) detecting, preventing and responding to intrusions; (iii) protecting against unauthorized access to/use of private information and (iv) disposing of private information within a reasonable amount of time after it is no longer needed for business purposes so that the information cannot be read or reconstructed.

Arent Fox

Letter Agreement between Zoom and the New York Attorney General (NYAG)

Following numerous reports of data security issues, NYAG investigated Zoom Video Communications, Inc. (“Zoom”):

- Found a “2000% increase” in Zoom users from January – March 2020 due to the COVD-19 pandemic
- Identified data security and privacy concerns that Zoom “acted to quickly to address”
  - Speedy response viewed as a mitigating factor (*c.f.* First American Title Insurance Company Notice of Charges)
- Zoom’s Head of Security will continue to implement, and maintain a comprehensive information security program (“Information Security Program”) that is reasonably designed to protect the security, confidentiality, and integrity of personal information that Zoom collects, receives, or processes

Arent Fox

Letter Agreement between Zoom and the New York Attorney General (NYAG)

Per the Letter Agreement:

- "Zoom shall employ reasonable encryption and security protocols, including by encrypting all personal information at rest in persistent storage on its cloud servers and by encrypting all personal information in transit except where the user fails to utilize a Zoom app or Zoom software for the transmission. Zoom will update and upgrade its security and encryption as industry standards evolve."
- "Zoom shall develop and maintain reasonable procedures to address credential stuffing attacks."

https://ag.ny.gov/sites/default/files/nyag_zoom_letter_agreement_final_counter-signed.pdf (last accessed August 26, 2020)

Arent Fox

State of New York, by Attorney General Letitia James v. Dunkin' Brands, Inc.

In a September 2019 complaint, the New York Attorney General alleges that Dunkin Donuts repeatedly failed to monitor and remediate deficiencies after a third-party developer reported repeated security breaches.

https://ag.ny.gov/sites/default/files/dunkin_complaint.pdf (*last accessed August 30 2020*)

Arent Fox

Other Recent State Data Security Enforcement

Other state enforcement with similar requirements:

- Press Release, Office of Attorney General Maura Healey, Online Sock Retailer Resolves Claims of Violating Data Security Laws)(Aug. 12, 2019) (**Bombas**)
- *Pennsylvania v. Orbitz Worldwide, Inc.*, Assurance of Voluntary Compliance (C.P. Phila. Dec. 13, 2019)(**Orbitz**)
- *D.C. v. Uber Technologies*, Final Judgment and Consent Decree, Civil Action No. 18- __ (D.C. Super. Ct. Sept 26, 2018)(**Uber**)

Arent Fox

Ohio's Data Security Law (Ohio Rev. Code § 1354.01)

Ohio's data security law offers an affirmative defense to a tort claim that failure to "implement reasonable information security controls" results in a data breach but only if the defendant can demonstrate that it "reasonably conforms" to one of the enumerated "industry recognized" cybersecurity frameworks:

- National Institute of Standards and Technology (**NIST**)
- Federal Risk and Authorization Management Program (**FEDRAMP**)
- International Organization For Standardization/International Electrotechnical Commission 27000 Family - Information Security Management Systems (**ISO 27001**)
- Payment Card Industry Data Security Standard (**PCI-DSS**)
- Center For Internet Security Critical Security Controls For Effective Cyber Defense (**CIS Controls**)

Arent Fox

California Consumer Privacy Act of 2018 (CCPA)

"Any consumer whose nonencrypted and nonredacted personal information[…] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information…" *AFTER* a 30-day cure period (CCPA §1798.150, 155)

- Statutory damages are limited to the greater of $750 per consumer per incident and actual damages
- Private right of action
  - 5+ consolidated class actions based in whole or in part on allegedly 'unreasonable' data security practices

General Data Protection Regulation (GDPR)

Compare an “omnibus” data security law:

“Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement *appropriate technical and organisational measures* to ensure a level of security *appropriate to the risk*…”

Article 32 of E.U. Regulation 2016/679

Arent Fox

GDPR's "Appropriate" Security Measures

- Encryption
- Pseudonymization
- Business Continuity/Disaster Recovery
- "Regularly testing, assessing and evaluating the effectiveness of technical and organisational measures"
- Evaluating processors (aka vendors)

Article 32 of E.U. Regulation 2016/679

Arent Fox

Assessing Reasonableness

Guideposts for Counsel

Arent Fox

Key Components of Reasonable Data Security

Common Requirements from the FTC and States

Arent Fox

1. Risks Assessments

What: A business must continually assess internal and external risks to the security, confidentiality and integrity of personal and confidential information

How: **At least annually**

FTC: Conducts risk assessments at least annually and within 30 days following data security-related events, together with security program updates to reflect the risk assessments (2019 i-Dressup order)

State:

- Engage an independent third party to conduct at least annual risk assessments (Equifax and Orbitz); use a third party who/that is a CISSP, CISA or similarly qualified, with 5+ years of risk assessment experience (Uber and Bombas)
- Massachusetts data security regulations (minimum general requirement #2: Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks,)
- New York SHIELD Act (administrative, physical and technical safeguard)

See Appendix for citations

Arent Fox

2. Testing and Monitoring

What: A business must monitor and test data security measures to ensure effectiveness.

How:

FTC:

- Called out businesses for failing to use "readily available" tools for monitoring, access control, patching and encryption (D-Link)
- FTC's June 2020 cloud security guidance: "**take advantage of the security features offered by cloud service companies**"
- In Tapplock, FTC requires **network vulnerability testing every four months** and **annual network penetration testing with test repeats within 30 days after a data security–related event**.

State:

- NY Attorney General called out Dunkin Donuts for repeatedly failing to monitor and remediate deficiencies after a third-party developer reported repeated security breaches

Arent Fox

3. Accountability

What: A business must assign responsibility for the data security program and ensure adequate oversight.

How:

FTC: In Tapplock, the FTC clarified that a "qualified" employee must oversee the data security program and deliver a written status report to the board and management "at least once every twelve months" and "promptly" after a data security–related event.

State:

- Equifax (Indiana) and Orbitz are required to not only hire a senior executive responsible for data security but also ensure that the executive receives necessary resources and provides quarterly Board reports.
- Massachusetts data security regulations (minimum general requirement #1: designation of one or more employees responsible for the WISP)
- New York SHIELD Act (administrative safeguard: designating one or more employees to coordinate the security program)

Arent Fox

4. Training

What: A business must train employees in both the threats identified in data security risk assessments and the safeguards intended to address those threats.

How:

FTC: In 2019 enforcement orders, the FTC specified annual employee data security training (Lightyear) and, for personnel involved with software development, biennial security training (D-Link).

State:

- Uber must deploy ongoing training for employees and contractors, together with disciplinary measures (including termination) for violations. Equifax must provide specialized training for all security personnel on personal information protection and the terms of the settlement prior to starting their responsibilities.
- Massachusetts data security regulations (minimum general requirement #2)
- New York SHIELD Act (administrative safeguard)

Arent Fox

5. Vendor Management

What: A business must not only select vendors capable of safeguarding data but also contractually obligate those vendors to maintain the safeguards but also verify their compliance with the contractual requirements.

How:

FTC: In the June 2020 cloud security guidance, the FTC reminds businesses that, even when outsourcing, “if it’s your data, it’s ultimately your responsibility”.

State:

- Equifax must contractually require vendors to notify Equifax within 72 hours after discovering a security incident.
- Massachusetts data security regulations(minimum general requirement #5)
- New York SHIELD Act (administrative safeguard)

Arent Fox

Other Common Security Requirements in Federal and State Enforcement

- Encryption of sensitive personal information stored on a business' network (Retina-X Studios)
- Encryption of all personal information at rest and in transit; security protocols upgraded "as industry standards evolve"; procedures to address credential stuffing attacks; and a program to discover and fix vulnerabilities (Orbitz; these types of specific security controls also are reflected in other state settlements)
- Network segmentation to separate sensitive information (Infotrax)
- Data access controls for personal information, including strong passwords and authentication, restricting inbound connections to approved IP addresses, limiting employees' access to the data they need to perform their job functions, deploying data loss prevention tools and inventorying devices connected to the business' network and ensuring the devices are securely installed (Lightyear and Tapplock)
- Tools for detecting unknown file uploads, limiting the locations to which third parties can upload files on business' network and monitoring network file integrity (Infotrax)

Arent Fox

Common Industry Data Security Standards

Arent Fox

NIST Cybersecurity Framework

Arent Fox

Other Industry Data Security Standards

- Center for Internet Security's Critical Security Controls (**CIS Controls**)
  - https://www.cisecurity.org/controls/cis-controls-list/
- Federal Risk and Authorization Management Program (**FedRAMP**)
  - https://www.fedramp.gov/documents/
- ISO 27001 Information Security Management System (**ISO 27001**)
  - https://www.iso.org/isoiec-27001-information-security.html
- Payment Card Industry Data Security Standards (**PCI-DSS**)
  - https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

Arent Fox

Industry Data Security Standards

How do industry standards answer the reasonable securitychallenge?

Pros	Cons
• Clear and specific requirements against which to benchmark • Recognized/recognizable by customers, regulators	• Resource-intensive • Expensive

Arent Fox

Wrapping Up

- General data security laws are designed for flexibility to accommodate varying business needs, resources and risk tolerance but are becoming increasingly specific.
- Nonetheless, the lack of definitive guidance creates challenges for attorneys advising data security professionals, boards and management who want “an answer” to what constitutes legally-required data security practices.
- Enforcement actions (federal and state) help to clarify regulatory expectations and perhaps also to limit the risk of a class action lawsuit.
- An industry data security standard offers a more definitive answer to the “reasonable” security question but also requires that a business have sufficient resources for certification to and/or demonstrable and ongoing compliance with the standard.

Arent Fox

Questions?

Contact

Julia Jacobson
Partner
617.549.1055
Julia.Jacobson@arentfox.com

Natalia Kerr
Attorney
845.521.9591

Arent Fox

Appendix

Arent Fox

Federal Laws

Gramm-Leach-Bliley Act (Public Law 106 – 102), https://www.govinfo.gov/app/details/PLAW-106publ102

- 15 U.S. Code § 6801: Protection of nonpublic personal information - requires Federal banking agencies, FTC and other regulators, to issue regulations ensuring that financial institutions protect the privacy of consumers' personal financial information, https://www.govinfo.gov/content/pkg/USCODE-2012-title15/pdf/USCODE-2012-title15-chap94-subchapI.pdf
- CFR Part 314: Standards For Safeguarding Customer Information
  ("This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. This part refers to such entities as "you." This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you."), https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=e2888177d956e8977ff3a5eff43a8b37&ty=HTML&h=L&mc=true&n=pt16.1.314&r=PART#se16.1.314_11

(last accessed August 27, 2020)

Arent Fox

DEFEND TRADE SECRETS ACT

Defend Trade Secrets Act (18 U.S.C. § 1836)

" … "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—**(A)** the owner thereof has taken reasonable measures to keep such information secret …"

Arent Fox

FTC DATA SECURITY ENFORCEMENT: 2019-2020 (*in alpha order*)

James V. Grago, Jr., individually and d/b/a ClixSense.com, Docket No. C-4678 (F.T.C. July 2, 2019*),* https://www.ftc.gov/system/files/documents/cases/172_3003_clixsense_decision_and_order_7-2-19.pdf (**ClixSense**)

F.T.C. v. D-Link Sys., Inc. Case No. 3:17-CV-39-JD (N.D. Cal. July 2, 2019), https://www.ftc.gov/system/files/documents/cases/dlink_proposed_order_and_judgment_7-2-19.pdf (**D-Link**)

- *See also* Complaint at 5, D-Link, https://www.ftc.gov/system/files/documents/cases/d-link_complaint_for_permanent_injunction_and_other_equitable_relief_unredacted_version_seal_lifted_-_3-20-17.pdf ("Defendants have failed to use free software, available since at least 2008, to secure users' mobile app login credentials, and instead have stored those credentials in clear, readable text on a user's mobile device.")

United States v. Unixiz, Inc., Case No. 5:19-cv-2222 (N.D. Cal. April 24, 2019), https://www.ftc.gov/system/files/documents/cases/i-dressup_stipulated_order_ecf_4-24-19.pdf (**i-Dressup**)

InfoTrax Sys., L.C., Docket No. C-4696 (*F.T.C.* January 6, 2020), https://www.ftc.gov/system/files/documents/cases/c-4696_162_3130_infotrax_order_clean.pdf (**InfoTrax**)

Arent Fox

FTC DATA SECURITY ENFORCEMENT: 2019-2020 (*in alpha order*)

LightYear Dealer Techs., LLC, *Docket No.* C-4687 (*F.T.C.* September 6, 2019), https://www.ftc.gov/system/files/documents/cases/172_3051_c-4687_dealerbuilt_decision_order.pdf (**LightYear**)

Retina-X Studios, LLC, Docket No. C-4711 (*F.T.C.* March 27, 2020), https://www.ftc.gov/system/files/documents/cases/1723118retinaxorder_0.pdf (**Retina-X Studios**)

United States v. Rockyou, Inc., Case No. 12-CV-1487 (N.D. Cal. March 28, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyouorder.pdf (**Rockyou**)

Tapplock, Inc., File No. 192 3011 (*F.T.C*. May 18, 2020), https://www.ftc.gov/system/files/documents/cases/192_3011_tapplock_agreement_containing_consent_order.pdf (**Tapplock**)

Arent Fox

NOTABLE FTC DATA SECURITY ENFORCEMENT: 2000-2019 (*chron order*)

F.T.C. v. Sandra L. Rennert, Civ. Action No.CV-S-00-0861-JBR (D. Nev. July 12, 2000) (*alleging that the defendants' false representation "expressly or by implication, that the information customers provide to their Web sites is encrypted and that defendants use an SSL secure connection when transmitting this information over the Internet" constitutes a deceptive act or practice, in violation of Section 5(a) of the FTC Act*)

BJ's Wholesale Club, Inc., Docket No. C-4148 (F.T.C. Decision and Order Sept. 20, 2005) (*alleging that failure to employ reasonable and appropriate security measures is an unfair act or practice*)
https://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter

United States v. Rockyou, Inc., Case No. 12-CV-1487 (N.D. Cal. March 28, 2012)
https://www.ftc.gov/sites/default/files/documents/cases/2012/03/120327rockyouorder.pdf

FTC v. Wyndham Worldwide Corp., Wyndham Hotel Group, LLC, Wyndham Hotels & Resorts, LLC, and Wyndham Hotel Management, Inc., Civil Action No. 2:12-cv-01265-SPL (D.N.J. 2012)
https://www.ftc.gov/enforcement/cases-proceedings/1023142-x120032/wyndham-worldwide-corporation

Arent Fox

NOTABLE FTC DATA SECURITY ENFORCEMENT: 2000-2019 (*chron order*)

TRENDnet, Inc., Docket No. C-4426 (*F.T.C.* Feb. 7, 2014), www.ftc.gov/system/files/documents/cases/140207trendnetdo.pdf

ASUSTeK Comput. Inc., Docket No. C-4587 (*F.T.C.* July 28, 2016), www.ftc.gov/system/files/documents/cases/1607asustekdo.pdf

LabMD, Inc. v. F.T.C., 894 F.3d 1221, 1229 (11th Cir. June 6, 2018), which vacates LabMD, Inc., Docket No. 9357 (F.T.C. July 28, 2016)

Complaint For Permanent Injunction And Other Equitable Relief, *F.T.C. v. Ruby Corp*., Case 1:16-cv-02438 (D.D.C Dec. 14, 2016), www.ftc.gov/system/files/documents/cases/161214ashleymadisoncmplt1.pdf

(last accessed August 27, 2020)

Arent Fox

KEY FTC DATA SECURITY GUIDANCE AND OTHER MATERIAL

FTC's Use of Its Authorities to Protect Consumer Privacy and Security (June 19, 2020), https://www.ftc.gov/news-events/press-releases/2020/06/ftc-issues-two-reports-requested-fiscal-year-2020-spending-bill

Six steps toward more secure cloud computing (June 15, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/06/six-steps-toward-more-secure-cloud-computing?utm_source=govdelivery

Stick with Security: A Business Blog Series (2017), https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series

App Developers: Start with Security (2017), https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security

(last accessed August 27, 2020)

Arent Fox

KEY FTC DATA SECURITY GUIDANCE AND OTHER MATERIAL

Protecting Personal Information: A Guide for Business (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

Careful Connections: Building Security in the Internet of Things (2015), https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things

Start with Security: A Guide for Business (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

Cybersecurity for Small Businesses, https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity (resource page developed in partnership with the National Institute of Standards and Technology, U.S. Small Business Administration and the Department of Homeland Security)

See also https://www.ftc.gov/consumer-protection/data-security

(last accessed August 27, 2020)

Arent Fox

NEW YORK DEPARTMENT OF FINANCIAL SERVICES (NYDFS) CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

23 NYCRR Part 500: https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf

FAQs: 23 NYCRR Part 500 – Cybersecurity:
https://www.dfs.ny.gov/industry_guidance/cyber_faqs

(last accessed August 27, 2020)

Arent Fox

INSURANCE DATA SECURITY MODEL LAW

Insurance Data Security Model Laws by the National Association of Insurance Commissioners (Model Regulation Service-4th Quarter 2017)

"Section 2: Purpose and Intent

A. The purpose and intent of this Act is to establish standards for data security and standards for the investigation of and notification to the Commissioner of a Cybersecurity Event applicable to Licensees, as defined in Section 3.
B. This Act may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act."

https://www.naic.org/documents/cmte_legislative_liaison_brief_data_security_model_law.pdf
(last accessed August 27, 2020)

Arent Fox

INSURANCE DATA SECURITY LAWS

Michigan Data Security Act (Public Act 690 of 2018) - passed on December 28, 2018 with a phased implementation schedule
http://www.legislature.mi.gov/documents/2017-2018/publicact/pdf/2018-PA-0690.pdf

New Hampshire Insurance Data Security Law (Chapter 420-P) - effective Jan 1, 2020 with a phased implementation schedule
https://www.gencourt.state.nh.us/rsa/html/XXXVII/420-P/420-P-mrg.htm

See also https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx

(last accessed August 27, 2020)

Arent Fox

Massachusetts Data Security Law and Regulations

- Law: https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H/Section2
- Regulations: https://www.mass.gov/regulations/201-CMR-17-standards-for-the-protection-of-personal-information-of-residents-of-the

SELECT STATE DATA SECURITY LAWS

- Del. Code Ann. tit. 6, § 12B-100 (2018) (“Any person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.”)
- Ark. Code Ann. § 4-110-104(b) (2018), Kan. Stat. Ann. 50-6, 139b (2017) (“A holder of personal information shall: (1) Implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure.”)
- Tex. Bus. Corp. Act Ann. Art. 521.052 (2009) (“A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business.”)
- Utah Code Ann. § 13-44-201 (2019) (“Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person.”)