Data Privacy and Cybersecurity New Laws and Regulations

Throughout 2022, we continue to see regulators placing an emphasis on the importance of protecting and securing information, in particular consumer personal information, at both the federal and state levels. Companies operating in the U.S. should assess their data privacy and cybersecurity practices and implement changes to meet these new laws and regulations starting in early 2023. For our clients navigating these complex requirements, we are pleased to share our Data Privacy and Cybersecurity report providing guidance on several of the most important developments including the New York Department of Financial Services new cybersecurity regulations, new U.S. state privacy laws, and the SEC's Proposed Cybersecurity Rules. We also provide practical guidance for how companies should prepare for all of these changes before the end of the year.

PAUL
HASTINGS

What Companies Need to Know about the New York Department of Financial Services ("NYDFS") Cybersecurity Regulation

On March 1, 2017, New York's Department of Financial Services ("NYDFS") implemented a comprehensive cybersecurity regulation aimed at financial institutions (the "Cybersecurity Regulation"). NYDFS has already brought a number of enforcement actions under the regulation resulting in multi-million dollar consent orders, and with the proposed amendments to the regulation that were introduced on July 29, 2022, the prevalence of these types of actions will likely continue.

At bottom, the Cybersecurity Regulation requires any company that is licensed under NYDFS—such as money transmitters and recipients of bit-licenses—to implement and maintain a comprehensive written cybersecurity program that is designed to protect the company's information systems and any non-public personal information stored on those systems. Among its many requirements, the Cybersecurity Regulation mandates that companies carry out and document a periodic risk assessment of their cybersecurity program, and establish policies and procedures governing information security, data governance, asset inventory, access controls, disaster recovery, incident response, and third party service provider management. In addition, the Cybersecurity Regulation requires companies to appoint an individual responsible for oversight of the cybersecurity program, appropriately staff and train its cybersecurity roles, implement encryption or other controls, and perform annual penetration tests on its environment.

To date, NYDFS has demonstrated a commitment to aggressively enforce the Cybersecurity Regulation, including a recent $30 million settlement with a crypto company, a $5 million settlement with an international cruise line, and a $3 million settlement with a life insurance company. With proposed amendments to the Regulation recently announced, high dollar enforcement actions will likely only increase.

In July of 2022, the NYDFS's Superintendent announced that NYDFS was considering several amendments to the Cybersecurity Regulation. NYDFS posted the amendment during a public comment period that ran from July 29 to August 18, 2022. If adopted as presently drafted, the amendment would implement a number of key changes, including those summarized below:

Topic Area	Key Aspects of Change
Heightened requirements for "large" companies.	The proposed amendment introduces "Class A Companies," which are NYDFS-regulated businesses that either (a) have over 2,000 employees, or (b) have over $1Bn in gross annual revenue, in each case including the company's affiliates. Class A Companies would be subject to heightened requirements, such as independent audits, endpoint detection requirements, and weekly vulnerability assessments.
New policy requirements	New policy requirements, including end-of-life management, remote access, and vulnerability and patch management would be required under the amendments. These (and the remaining policies mandated by the Cybersecurity Regulation) must be approved annually by a senior governing body.
CISO Independence and Reporting	The covered entity's CISO must have "adequate independence" and authority to "ensure cybersecurity risks are appropriately managed." In the annual report mandated by the existing Cybersecurity Regulation, the proposed amendments require that the CISO additionally discuss plans for remediation of identified deficiencies related to the Company's cybersecurity program.
Limitations and oversight of privileged accounts	The proposed amendments additionally introduce a number of new technical safeguards that covered entities would be required to implement, including limitations on the number and use of privileged accounts, a "password vaulting solution" for privileged accounts, and the use of multi-factor authentication for privileged accounts.
Risk assessment cadence	The proposed amendments would require covered entities to perform a risk assessment annually, instead of "periodically."
Additional requirements for business continuity and disaster recovery plans	The proposed amendments introduce a number of new requirements related to business continuity and disaster recovery plans, including the identification of essential data, facilities, infrastructure, and personnel; a communications plan; and procedures for maintenance of back-up facilities. The amendments also require that covered entities maintain backups that are isolated from network connections.
Breach notification threshold	The proposed amendments require that a covered entity notify NYDFS within 24 hours of any "extortion payment," and, thirty days thereafter, provide a written description of the reasons that the payment was necessary, the alternatives that were considered, and the diligence that was performed with respect to the incident to ensure compliance with applicable law.

Key Takeaway – Companies operating in the financial sector that are subject to NYDFS jurisdiction should begin preparing for these changes now. Although the proposed amendment may be modified to some extent prior to becoming final, the thrust of these new requirements will likely remain the same, and NYDFS has demonstrated that it is ready and willing to bring enforcement actions against perceived violators. To prepare for these changes, companies subject to NYDFS oversight should review their cybersecurity policies, procedures, and practices with counsel and begin prioritizing compliance efforts.

PAUL
HASTINGS

New Comprehensive U.S. State Privacy Laws are Coming – Is Your Company Ready?

Over the last two years, many states have taken cues from California and the EU by adopting sweeping privacy laws. These laws, passed in Virginia, Colorado, Connecticut and Utah, as well as updates to the already enacted California Consumer Privacy Act ("CCPA"), are focused on providing consumers (and soon employees in some states) better information about how their data is used, more control over their data and imposing additional requirements on companies to protect consumer personal information.

Similarities and Differences in the New Laws

While each law should be reviewed to understand their specific requirements, each has similar provisions related to requiring companies to

- Implement reasonable security measures;
- Share data with third parties only when those third parties are subject to specific contractual requirements limiting their own uses of the data;
- Provide clear privacy notices that must include details of the collection and use of data; and
- Most of the new laws also give state regulators broad authority to pursue enforcements for violations of the law

It is important to note that even though there are similarities, the laws also have important, and often nuanced, differences that companies must understand in order to comply with the laws' requirements. Below, are some of the more significant differences:

	CA	VA	CO	CT	UT
Consumer Rights[1]	Yes, but right to confirm processing is not explicitly included	Yes	Yes	Yes	Yes, but no right to correction
Right to opt out of certain processing	Sale of PI Sharing for contextual advertising	Targeted advertising Sale of PI Profiling	Targeted advertising Sale of PI Profiling	Targeted advertising Sale of PI Profiling	Targeted advertising Sale of PI
Applies to Employees	Yes	No	No	No	No
Applies to B2B Data	Yes	No	No	No	No
Do HIPAA Exemptions Apply?	Yes, but only HIPAA data is exempted	Entities subject to HIPAA exempted	Entities subject to HIPAA exempted	Entities subject to HIPAA exempted	Entities subject to HIPAA exempted
Do GLBA Exemptions Apply?	Yes, but only GLBA data is exempted	Entities subject to GLBA exempted	Entities subject to GLBA exempted	Entities subject to GLBA exempted	Entities subject to GLBA exempted
Private Right of Action	Yes, but only for data breaches	No	No	No	No
Privacy Assessments	Yes	Yes	Yes	Yes	No

1. Except where otherwise indicated in this chart, the following consumer rights are included in these laws: confirm processing, access, portability, correction, deletion, and equal services and price

Effective Dates

The laws will come into effect throughout 2023. In particular the laws become effective on:

- The California Privacy Rights Act — January 1, 2023.
- The Virginia Consumer Data Protection Act — January 1, 2023.
- The Colorado Privacy Act — July 1, 2023.
- The Connecticut Data Privacy Act — July 1, 2023.
- The Utah Consumer Privacy Act —- December 31, 2023.

What Companies Should be Doing to Prepare

As an initial matter, companies that are subject to these laws must assess their current practices to determine whether they meet the law's specific requirements. Where there are gaps, companies should focus first on California and Virginia requirements (which come into force first) and should work to remediate those gaps before the end of this year.

We recommend that companies focus on the following:

1. ***Determine whether these laws apply to your company***

   The following are the thresholds for each state:

   - **California:** $25 million in annual gross revenue in the preceding calendar year; or processes data of at least 100,000 consumers; or derives at least 50% of gross revenues from selling or sharing data.
   - **Virginia:** Processes data of at least 100,000 consumers; or processes data of at least 25,000 consumers and derives at least 50% of gross revenues from selling data.
   - **Colorado:** Processes data of at least 100,000 consumers; or processes data of at least 25,000 consumers and derives revenue or receives a discount on goods or services from selling personal data.
   - **Connecticut:** Processes data of at least 100,000 consumers (excluding purely payment transactions); or processes data of at least 25,000 consumers and derives at least 50% of gross revenues from selling personal data.
   - **Utah:** $25 million in annual gross revenue; and processes data of at least 100,000 consumers; or processes data of at least 25,000 consumers and derives at least 50% of gross revenues from selling personal data.

2. ***Review and update privacy notices and privacy rights links.*** Companies should review and update, as needed, their privacy notices (including website privacy policies, internal privacy policies, and other just-in-time collection notices) to reflect the new state law requirements.
3. ***Review your online advertising practices.*** Companies that process personal data from website visitors for the purposes of targeted advertising should also review the state requirements that allow visitors to opt-out via a universal opt-out mechanism or global privacy control.
4. ***Review your uses of sensitive data.*** While companies may be familiar with the requirements for special categories of personal data as defined under the GDPR, several of the new state privacy laws also provide specific requirements for the use and disclosure of "sensitive personal information."
5. ***Implement privacy assessments.*** California, Virginia, Colorado and Connecticut require a data protection assessment for certain activities, including those that involve the use of sensitive personal information or other "high-risk" data.
6. **Review consumer privacy rights requests procedures.** Companies will need to update their internal consumer privacy rights requests processes to address the new state privacy rights, including in California to address employee and business-to-business contact rights requests.
7. **Review and update vendor agreements.** Companies should review and update their vendor agreements involving personal data to ensure they meet the requirements of the new state privacy laws and to ensure vendors are also bound to such requirements.
8. **Provide training to employees.** Employees from compliance, HR, and marketing as well as those who implement the technical business requirements for privacy compliance need to be trained on the new state privacy laws.

PAUL
HASTINGS

SEC Proposed Cybersecurity Rules – What They are and What Our Clients Should be Doing Now

What are the New Rules?

Earlier this year, the Securities and Exchange Commission (SEC) published a new set of proposed cybersecurity disclosure rules for public companies. The proposed rules would significantly increase SEC scrutiny of public companies' cybersecurity-related business activities, decision-making processes and the Board's new role in overseeing cybersecurity.

These proposed rules signal the increasing importance the SEC places on cybersecurity, going farther than any federal agency to date in placing obligations on public companies and their Boards of Directors. One of the most significant new obligations requires public company Board oversight and involvement in the review, assessment, and implementation of cybersecurity policies and procedures. The proposed rules also create stronger and more uniform guidelines for companies regarding disclosures, and ongoing supplementation, of "material" cybersecurity incidents.

The comment period for these rules originally ended on May 9, 2022, with hundreds of comments submitted. However, the SEC recently reopened the comment period for an additional 14 days due to a technical error that may have caused issues with public comments submitted through the SEC's website.

While we do not yet have a date for when the rules will be finalized or effective, the Office of Management Budget indicated that final action will be taken in April 2023. Given the significant changes that are likely to be included in the new rules, companies and their boards should take steps to prepare now.

What are Some of the Key Requirements if the Rules are Adopted?

- If the SEC adopts the rules similar to their proposed form, the key obligations include:
- Report "material cybersecurity incidents" to the SEC within 4 days;
- Report non-material incidents that, when combined with other incidents, become material "in the aggregate";
- Provide updates on prior incidents in periodic SEC disclosures;
- Provide a description of the company's cybersecurity risk management system;
- Describe the Board's oversight of cybersecurity risk; and
- Disclose the cybersecurity expertise of the Board members.

What is Changing from the Current Rules?

- ***Companies and their senior leadership will be held to a higher standard.*** Under the new rules, companies will be required to develop and maintain reasonable cybersecurity practices, describe those practices in public filings, explain how their senior leadership oversee those programs effectively, and report cybersecurity incidents in a way that provides appropriate information to shareholders.
- ***The rules will be clearer (hopefully).*** While more granular and potentially burdensome than in the past, the new rules will provide clarity on and solidify earlier guidance and the outcomes of recent SEC enforcements. Current rules, guidance, and enforcements have created an inconsistent and potentially confusing standard for cybersecurity that will be remedied, at least in part, by these new rules.
- ***More, and more detailed, documentation will be required.*** Among the recent findings in various SEC enforcements is the clear message from the Commission that it believes that cybersecurity incident reports often lack detail, are inconsistent, and are not timely. The new rules provide guidelines for the content, timing, and format of incident reports and periodic disclosures. The new rules also require adequate documentation of companies' cybersecurity and risk management programs.

What Should Companies be Doing to Prepare?

- ***Review cybersecurity and risk management documents.*** Cybersecurity and risk management systems can take months to update. Companies should start reviewing and updating these programs now. Companies should pay particular attention to changes in their technology infrastructure, recent acquisitions and mergers, changes in the threat landscape, and lessons learned from any recent security incidents.
- ***Educate your Board.*** With all of the new requirements for oversight being placed on the Board, the Board will need to ensure that it is prepared to oversee the cybersecurity and risk management policies and procedures of the company. However, few Boards have historically been provided with enough detail to take on this task. Determine whether the full Board, or a subset of the Board, will be primarily responsible for oversight, ensure that they have been properly educated and approve of the company's policies and procedures.
- ***Review your incident response plans.*** All companies should have an incident response plan, but we recommend a review of such plan in light of these new proposed rules. Your incident response team should be aware of this timeline and know whether and how to escalate as needed. The incident response plan should also have a clear escalation plan for raising significant or material incidents with senior leadership and the Board. The window for reporting a material incident to the SEC is 4 days – that is a shorter notification period than any other US law. Like the other cybersecurity policies and procedures, the Board should be educated on the incident response plan and then participate in a table top exercise to simulate a real incident.
- ***Identify what materiality means to your company.*** Any decision on the materiality of an incident, which would require notification within 4 days, should be made by the company's legal team and the senior leadership as appropriate. The Company should specifically ensure that both the incident response plan and operating environment have the appropriate procedures for escalation to the legal team and senior management who will make the materiality determinations.

Our Data Privacy and Cybersecurity practice regularly advises companies on how to meet the requirements of new laws. If you have any questions concerning these new laws and regulations starting in early 2023 or any other data privacy or cybersecurity laws, please do not hesitate to contact any member of our team.

Paul Hastings Data Privacy and Cybersecurity Team

Paul Hastings Privacy and Cybersecurity Solutions Group