March 2020

PRIVACY AND DATA SECURITY CLIENT ALERT

SHOOK HARDY & BACON

The link to Shook's initial guidance on the CCPA modified draft regulations has been corrected below. We apologize for the inconvenience.

SUBSCRIBE

ARCHIVE

CCPA

Shook Weighs in on Updated CCPA Regulations

In response to extensive public comment, the California Attorney General's office released modified draft regulations under the CCPA on February 7. Shook has provided initial guidance on the draft, which included a substantial number of changes.

TAKEAWAY

The modified regulations will impose a lighter compliance burden compared to their initial release. These regulations are likely to become effective July 1, 2020.

Class Action Complaint Cites CCPA

A data-breach putative class action filed against online retailer Hanna Andersson and Salesforce, its e-commerce platform, is seemingly the first to cite the California Consumer Protection Act (CCPA). While the original complaint didn't include a cause of action under the CCPA, the parties have stipulated to an amended complaint that does.

Beyond the novelty of a claim made under the CCPA, the amended complaint is interesting in two respects. First, while the original breach took place in 2019—before the CCPA went into effect—the amended complaint avoids that hurdle by alleging that "hackers further disclosed" personal information in 2020. Second, the

Shook, Hardy & Bacon understands that companies face challenges securing information in an increasingly electronic world.

Shook guides its clients through an ever-changing patchwork of data security and data privacy laws and regulations, and helps its clients manage litigation and other risks associated with maintaining and using electronic information.

To learn more about Shook's Privacy and Data Security capabilities, please visit shb.com or contact:

Al Saikali
Chair, Privacy and Data Security Practice
305.358.5171
asaikali@shb.com

amended complaint alleges that Hanna Andersson and Salesforce "failed to 'actually cure'" the violation of 1798.150 within 30 days of an alleged written notice. The amended complaint doesn't specify what form that notice took, nor exactly when it happened. It will be interesting to see if it becomes an issue in the case. For example, did plaintiff file suit under other causes of action while the CCPA notice period ran its course, knowing that she would amend her complaint after that period to add a claim under the CCPA? This case could be an important first step in judicial clarification of the CCPA.

TAKEAWAY

Plaintiffs are already beginning to test ways to incorporate the CCPA into complaints, even for events that took place before the law's effective date. Companies can expect those efforts to continue.

FTC

FTC Improves Data-Security Orders to Achieve Greater Privacy Compliance

Based on public feedback and lessons learned from the 2018 *LabMD* decision, the U.S. Federal Trade Commission (FTC) rolled out new and improved data-security orders—which have already been used in seven enforcement actions. The improvements fall into the following three categories:

1. **Increase specificity** – FTC orders must now specify the areas in which security is lacking and systems and process must be developed. For example, an order might now require access controls, yearly employee training or data encryption instead of simply requiring that a company "implement comprehensive data security systems and processes."
2. **Increase third-party assessor accountability** – FTC will now require its outside assessors to identify specific areas in which data security is lacking and support their findings with evidence. Third-party assessors will be required to retain documents related to assessments and cannot refuse to provide those documents to FTC on the basis of certain privileges, and allow FTC to force a company to hire a new assessor if a previous assessor fails to meet FTC approval.
3. **Elevate data security considerations to the C-Suite and Board Members** – Aiming to increase effective data privacy compliance, FTC will now require yearly presentations to boards and executives on a company's written security program. Data shows that governing bodies should be aware of cybersecurity issues a company faces.

TAKEAWAY

Colman McCarthy
Associate
816.559.2081
cdmccarthy@shb.com

Kate Paine
Associate
813.202.7151
kpaine@shb.com

Ben Patton
Associate
206.344.7625
bpatton@shb.com

Lischen Reeves
Associate
816.559.2056
lreeves@shb.com

Data privacy and security violations in 2020 and beyond will be met with strict FTC orders. Legal departments should keep abreast of what is required to stay compliant with privacy laws to avoid reprimand from FTC.

FTC Publishes Annual Privacy and Security Update

FTC has published "Privacy & Data Security Update: 2019" detailing various enforcement actions under its Section 5 authority, GLBA, FCRA, CAN-SPAM, and COPPA. Notably, FTC brought more than 130 spam and spyware cases, 80 "general privacy lawsuits" and more than 70 cases against companies for unfair and deceptive trade practices involving inadequate protection of consumers' personal data. Additionally, FTC collected more than $40 million in civil penalties from more than 100 FCRA violations. Lastly, FTC brought 64 actions under international privacy frameworks including 39 under the U.S.-EU Safe Harbor program, 4 under the APEC CBPR and 21 under Privacy Shield.

TAKEAWAY

FTC is showing no signs of slowing down its enforcement actions. Given the increase in public scrutiny on companies' privacy practices, expect FTC to continue to increase regulatory actions against companies to protect consumers' privacy and personal information.

HIPAA

OCR Aiming to Increase Compliance with Basic HIPAA Rules

Timothy Noonan, the deputy director for health information privacy at the Health and Human Services' Office of Civil Rights (OCR), shared his thoughts on HIPAA compliance and enforcement issues. One of the more notable of Noonan's comments was that OCR is working on proposed modifications to the HIPAA Privacy Rule to reduce regulatory burdens. He also discussed OCR's continued focus on ensuring patients have confidence and trust in the privacy and security of their health information and a new focus on a patient's right of access to medical records. On the latter topic, Noonan stated that right of access compliance failures are some of the most recurring. His comments tie in with those of OCR Director Roger Severino, who commented in an interview with *Law360* that HIPAA-covered entities continue to commit many **basic** HIPAA missteps, which his office sees as "low-hanging fruit ripe for enforcement." As of

January 2020, OCR has received more than 200,000 HIPAA Privacy Rule complaints and has obtained some form of corrective action in approximately 70% of all complaints. The following are common basic HIPPA violations:

1. Lack of comprehensive risk analyses
2. Failure to grant right of access when applicable and appropriate
3. Failure to implement access controls
4. Failure to implement proper password policies
5. Failure to conduct system activity reviews
6. Failure to conduct sufficient privacy training

TAKEAWAY

OCR is well aware of basic compliance failures and has signaled willingness to target those failures. HIPAA compliance begins with understanding the flow of data within an organization. Once at a point of understanding, a covered entity must take steps to fix any security vulnerabilities. Please contact Lischen Reeves with any questions about HIPAA.

OCR Issues Fine for HIPAA Security Rule Violations

A small medical facility agreed to pay $100,000 to OCR and adopt a corrective action plan after an investigation into a doctor's medical practice found that he had never conducted a risk analysis at the time he reported a data breach resulting in a potential violation of the HIPAA Security Rule. Despite significant technical assistance throughout the investigation, the doctor failed to complete an accurate and thorough risk analysis after the breach and failed to implement proper security measures.

TAKEAWAY

Businesses covered by HIPAA must perform risk analyses of their systems to avoid potential HIPAA Security Rule violations.

Potential New Privacy Framework for Health Data Not Protected by HIPAA

The Center for Democracy and Technology (CDT) and the eHealth Initiative (EHI) are collaborating to develop a privacy framework for health data in situations not covered under the HIPAA privacy and security rules, such as wellness apps and wearable devices. The effort, which includes leaders in health care, technology, and privacy and consumer advocacy, aims to increase protections for health-related data.

TAKEAWAY

With federal legislation seemingly always a long shot and state law a patchwork, industry self-regulation can be the best chance for a national approach to address gaps in current law.

Security Firm Warns of Insecure Storage Systems for Medical Providers

Security researchers have reportedly issued a warning to hundreds of hospitals and medical offices that patients' personal health information is being exposed on the internet due to unprotected servers. The issue stems from servers at medical facilities establishing connections to the internet without being secured by a password. As a result, if an insecure connection is found, anyone with an internet connection and free-to-download software can access medical images of patients across the world resulting in potential HIPAA violations by the medical facilities who have failed to secure their servers.

TAKEAWAY

Widely available software can make sharing health information among doctors easier, but it can expose data to greater risk of unauthorized access or disclosure. When paired with lax security (e.g., failing to secure databases connected to the internet), it can multiply the harmful effects.

INTERNATIONAL UPDATES

Irish DPC Report

The Irish Data Protection Commission (DPC) has released its 2019 Annual Report, which highlights the work DPC has completed in the first full calendar year since the General Data Protection Regulation (GDPR) went into effect on May 25, 2018.

DPC reports that since then, 49 Domestic Statutory Inquiries and 21 Multinational Technology Company Statutory Inquiries have commenced. DPC also received 75% more complaints in 2019 (7,215 versus 4,113 in 2018). But it remains efficient, resolving 5,496 total complaints in 2019. There were also 6,069 "valid" data-security breaches brought to DPC's attention in 2019, which is a 71% increase on 2018's number of 3,542.

DPC likely sees such a magnitude of cases because many major international technology and social-media companies have their "main establishment" in Ireland, making DPC the Lead Supervisory Authority. For questions about the GDPR, please contact Kate Paine.

TAKEAWAY

Ireland's DPC continues to be among the more prominent data-protection authorities in the EU, and staying current on its priorities will provide insight on important GDPR trends.

EU Regulator Releases Strategy on Cyber Underwriting

The EU's Insurance and Occupational Pensions Authority (EIOPA) is concerned about the resilience of the cyber-insurance market and the potential systemic risk to the financial system posed by cyberattacks. It has released a strategy document aimed at reducing that risk. Among the proposals EIOPA set out are creation of a centralized (and anonymized) database on cyber incidents, further investigation and guidance on non-affirmative or "silent" cyber risk, and inclusion of cyber-incident scenarios in EIOPA's stress-testing framework.

TAKEAWAY

Cyber insurance continues to grow in importance, and top regulators around the world are proactively taking steps to help the market as it matures.

STATE PRIVACY LAWS

South Carolina Introduces Comprehensive Biometric Privacy Bill

A bipartisan group of South Carolina lawmakers have taken a significant step to expand state privacy protections by introducing the South Carolina Biometric Data Privacy Act, a bill that borrows from both Illinois BIPA and the CCPA. Like BIPA, it would require notice and consent before collection of biometric information, and it provides a private right of action and statutory damages for a person "aggrieved" by a violation. Like the CCPA, the bill would provide consumers with certain rights in connection with their biometric information, such as rights of access and deletion and the right to opt out of the sale of biometric information.

And as an additional kicker, the bill includes a breach-notification provision that would require notification to consumers within 72 hours of a breach of "business data" (undefined by the bill)—with a $5,000 fine for *each* consumer that was not notified.

TAKEAWAY

If this South Carolina bill passes, it will be the strictest biometric-privacy law in the country, with the highest exposure for violations. More than 50 privacy bills are under consideration at

the state level. Shook's clients may contact Colman McCarthy to receive our weekly tracker of privacy legislation.