Originally published by
Law360
A LexisNexis® Company

CULHANE MEADOWS PLLC

Early Lessons From Enforcement Of Calif., NY Privacy Laws

By **Caroline Morgan** (September 28, 2020)


Caroline Morgan

In 2020 two powerful privacy laws came into effect, the California Consumer Privacy Act and New York's Stop Hacks and Improve Electronic Data Security Act.

Generally, the CCPA provides consumers with access to and control over their personal information that businesses collect. The SHIELD Act protects the private information of New York residents by imposing data breach notification and data security program requirements on companies.

Businesses can avoid hefty fines and reputational harm by learning how the attorney general of each state has enforced their new law.

The SHIELD Act can apply to a company that is not doing business in New York.

Before delving into early enforcement actions, it is worthwhile to dispel the common misconception that the SHIELD Act only applies to New York businesses. It is true that the purpose of the SHIELD Act is to protect the private information of New York residents; however, it applies to a company wherever it conducts business so long as it owns or licenses the private information of a single New York resident.

Given this expansive territorial range coupled with its substantial penalties including up to $250,000 for breach notification violations and an uncapped amount for violation of its data security standards, a business's compliance strategy will undoubtedly be more robust if it determines whether the SHIELD Act applies to it in addition to the CCPA. With that we can now turn to early enforcement, as discussed below.

Learn from early CCPA noncompliance letters.

Last year, the California attorney general warned businesses that if they fail to comply with the CCPA he "will descend on them and make an example of them."[1] The CCPA went into effect this year and despite requests to postpone enforcement due to COVID-19, the California AG began enforcement on July 1 by issuing noncompliance letters to businesses. Although the recipients and contents of the letters are confidential, businesses can learn from recent statements made about the letters by Supervising Deputy AG Stacey Schesser.[2]

With a typical disclaimer that her views are not the views of the AG, Schesser confirmed the following about the noncompliance letters:

- The AG targeted multiple industries.

- The AG focused on businesses that operate online that were missing required statements including a "Do Not Sell My Personal Information" link on their homepage if they are selling personal information.

- The AG identified the businesses in part by reviewing their websites and consumer complaints, including those made on Twitter and other social media.

Given the above, businesses should not hold any false belief that their industry is immune from enforcement or that the AG is only focusing on a specific sector. In addition, companies can mitigate their exposure by verifying they have appropriate links on their websites and by reviewing customer complaints, including those posted on their social media, for any content related to the CCPA.

Further, according to Schesser, the California AG considers the following a priority for enforcement: violations concerning the personal information of minors and other vulnerable populations, health information, financial information, wide-scale violations that have a large impact on Californians, and any repeated customer complaints that the AG receives about a business. The AG's office is also purportedly taking note of class actions already filed pursuant to the CCPA's private right of action and may take enforcement actions based on them where appropriate.

Every business's goal is to avoid being a recipient of a noncompliance letter. But if a company receives a notice, how it responds becomes critical because it could dissuade the AG from filing a lawsuit.

Demonstrate a good faith effort to comply to avoid a CCPA investigation or lawsuit.

Under the CCPA, before the AG may bring an enforcement action, he must provide a business with notice of any alleged violation and an opportunity to cure them within 30 days. More than 30 days has passed since the AG issued the first noncompliance letters and he has not filed a lawsuit, which could be due in part to responses that demonstrate a good faith effort to comply.

The AG indicated he does not expect perfect compliance with the CCPA but "given that we are an agency with limited resources ... we will look kindly on those that ... demonstrate an effort to comply."[1]

Accordingly, businesses can benefit by showing how they have made a good faith effort to comply with the CCPA in response to a deficiency notice. In so doing, businesses can further mitigate their exposure because investigations initiated pursuant to a CCPA complaint may also implicate other laws like the California Online Privacy Protection Act, the Confidentiality of Medical Information Act, and California's Unfair Competition Law which could lead to greater exposure.

In addition to the CCPA, early enforcement actions have shed light onto compliance with the SHIELD Act.

Be guided by data security settlements following the SHIELD Act.

Last year, the New York attorney general declared the SHIELD Act "the law of the land" and vowed "companies will be held accountable for securing [New Yorkers'] information."[3] The second and final part of the SHIELD Act went into effect in March 2020, mandating businesses to develop, implement and maintain a data security program to protect private information on top of the first part's data breach notification requirements.

To date it appears the New York AG has not brought a lawsuit under the SHIELD Act, but because the AG is not required to give a business notice of its noncompliance like the CCPA, the lack of a lawsuit does not necessarily mean enforcement is lax. Since the SHIELD Act took effect, the AG has agreed to two settlements with Zoom Video Communications Inc. and Dunkin' Brands Group Inc. concerning their data security practices which are instructive on compliance.

Identify internal and external security risks and implement safeguards to control them.

In March, the New York AG opened an investigation into Zoom's privacy and data security practices after its use skyrocketed following COVID-19 lockdowns and users reported security flaws. On May 7, the AG announced Zoom's agreement to enhanced security measures removed the need to file a lawsuit.[4] As per the agreement, Zoom is required to have a comprehensive information security program with the following administrative, technical, and physical safeguards that expands on similar requirements in the SHIELD Act:

> Designation of an employee or employees to coordinate and be accountable for the information security program, whom shall report directly to [a] Head of Security;
>
> Identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks;
>
> Design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;
>
> Design and implementation of a security code review process to identify and remediate common security vulnerabilities; and
>
> Evaluation and adjustment of the information security program described herein in light of the results of the testing or monitoring required by these terms.[5]

In addition to the above, the settlement with Dunkin' details additional safeguards that a company should incorporate into its data security program.

Incorporate safeguards against credential stuffing and other common cyberattacks.

On Sept. 15, the AG announced Dunkin', franchisor of Dunkin' Donuts, agreed to pay $650,000 in penalties and costs to resolve a 2019 lawsuit concerning its alleged failure to respond to cyberattacks and to protect customer information. Pending court approval, the settlement also imposes affirmative obligations on Dunkin' including maintaining a comprehensive information security program that has reasonable technical, administrative, and physical safeguards required by the SHIELD Act.[6]

As per the AG's press release of the settlement, the safeguards should include measures to mitigate against frequent attack paths including credential stuffing.[7] Credential stuffing is a type of cyberattack where hackers use compromised credentials like usernames or passwords to access accounts relying on the assumption that people reuse their passwords. Notably, Zoom's settlement also requires it to develop and maintain reasonable procedures

to address credential stuffing.

Businesses must also develop and implement an incident response plan. In the context of credential stuffing, a business may have to conduct a reasonable investigation to identify affected customers and take appropriate action to protect them, like resetting passwords, freezing customers' accounts, or notifying customers their accounts have been compromised.

Takeaway

From missing a "Do Not Sell My Personal Information" link to customer complaints on a company's Twitter account, businesses can head off further investigation or a lawsuit by curing such violations in notices of noncompliance and demonstrating a good faith effort to comply with the CCPA.

To avoid liability under the SHIELD Act businesses should have a comprehensive data security program with appropriate technical, administrative and procedural safeguards, including those to minimize credential stuffing and other common cyberattacks.

By adopting the lessons learned from early enforcement actions, companies can reduce their exposure under the CCPA, the SHIELD Act, and each state's other laws that could be implicated by a business's weak data security practices.

Caroline A. Morgan is a partner at Culhane Meadows PLLC.

[1] https://www.reuters.com/article/us-usa-privacy-california/california-ag-says-privacy-law-enforcement-to-be-guided-by-willingness-to-comply-idUSKBN1YE2C4.

[2] https://iapp.org/news/a/iapp-summit-sessions-keynote-ccpa-enforcement-enter-the-ag/.

[3] https://ag.ny.gov/press-release/2019/attorney-general-james-statement-shield-act#:~:text=%25E2%2580%259CThe%2520SHIELD%2520Act%2520is%2520now,accountable%2520for%2520securing%2520their%2520information.

[4] https://ag.ny.gov/press-release/2020/attorney-general-james-secures-new-protections-security-safeguards-all-zoom-users.

[5] https://ag.ny.gov/sites/default/files/nyag_zoom_letter_agreement_final_counter-signed.pdf.

[6] https://ag.ny.gov/sites/default/files/proposed_consent_order_and_judgment.pdf.

[7] https://ag.ny.gov/press-release/2020/attorney-general-james-gets-dunkin-fill-holes-security-reimburse-hacked-customers.

The foregoing content is for informational purposes only and should not be relied upon as legal advice. Federal, state, and local laws can change rapidly and, therefore, this content may become obsolete or outdated. Please consult with an attorney of your choice to ensure you obtain the most current and accurate counsel about your particular situation.

About Culhane Meadows – *Big Law for the New Economy*®

The largest woman-owned national full-service business law firm in the U.S., Culhane Meadows fields over 70 partners in ten major markets across the country. Uniquely structured, the firm's Disruptive Law® business model gives attorneys greater work-life flexibility while delivering outstanding, partner-level legal services to major corporations and emerging companies across industry sectors more efficiently and cost-effectively than conventional law firms. Clients enjoy exceptional and highly-efficient legal services provided exclusively by partner-level attorneys with significant experience and training from large law firms or in-house legal departments of respected corporations. U.S. News & World Report has named Culhane Meadows among the country's "Best Law Firms" in its 2014 through 2020 rankings and many of the firm's partners are regularly recognized in Chambers, Super Lawyers, Best Lawyers and Martindale-Hubbell Peer Reviews.