Avoid Becoming a Target of Privacy and Data Breach Class Action Lawsuits

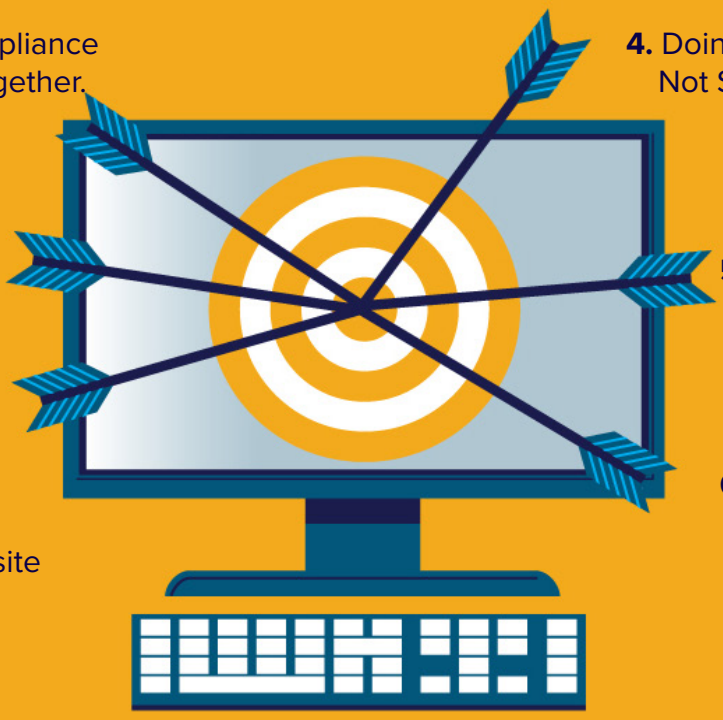
troutman sanders

A review of privacy and data breach class action lawsuits reveal an ongoing trend. Plaintiffs filing these actions, time and time again, rely on the same allegations concerning missteps taken by an organization in the areas of privacy and data security. Allegations usually range from a business failing to accurately disclose its data collection and sharing practices to an organization's failure to implement "reasonable security procedures." Even as the privacy landscape shifts and new laws, such as the California Consumer Privacy Act (CCPA), take effect, these basic allegations continue to be the foundation of every privacy and data breach class action lawsuit. For businesses looking to avoid becoming the target of one of these complaints, addressing the issues highlighted below is an easy way to start. Even better – these same issues, if avoided, can also serve as a defense to these same common privacy and data security-related claims.

1. Business and Compliance Failing to Work Together.

2. Adding "Feel-Good" Language to Privacy Notices.

3. Not Considering Mandatory Arbitration in Website Terms of Use.



4. Doing What You Say, but Not Saying What You Do.

5. Failing to Test Incident Response Plans.

6. Failing to Consider What "Reasonable Security Procedures" Requires.

1. Business and Compliance Failing to Work Together.

It is not uncommon for the functionality of a product to get ahead of an organization's privacy notices and disclosures. When this happens, businesses are often faced with claims that they have violated consumers' reasonable expectations of privacy. To avoid this, it is critical for business and compliance to work together to establish policies and practices that cover not only how the product is expected to operate today, but also how it may operate in the foreseeable future. This is especially important in light of the COVID-19 outbreak, which has significantly changed how certain products and services are being used (consider Zoom's video conferencing app, for example).

2. Adding "Feel-Good" Language to Privacy Notices.

The first quote in every privacy and data breach class action lawsuit is the "feel-good" language organizations include in their privacy notices to emphasize their commitment and dedication to privacy and data security. While this language may

make businesses look more appealing and consumer-friendly, plaintiffs are quick to pick up on this language and recite them back to the courts in their complaints. Unless there is a good reason to include this type of language in your privacy notice (there likely is not), businesses should filter out the fluff and instead stick to what is required.

3. Not Considering Mandatory Arbitration in Website Terms of Use.

Many businesses have been able to defeat privacy and data breach class action lawsuits by invoking the mandatory arbitrations provisions in their agreements and website terms of use. A mandatory arbitration provision may also create some interesting class issues (e.g., which class members are bound to the arbitration provision, which are not?). While adding a mandatory arbitration provision may not be appropriate in every situation, it is at least an issue worth considering before rolling out a new agreement.

4. Doing What You Say, but Not Saying What You Do.

Privacy-based class action lawsuits are littered with allegations that businesses failed to accurately disclose the extent of their data collection and sharing practices (consider the In re: Facebook Inc. Internet Tracking Litigation, which we reviewed in detail in our article, "Calif. Privacy Law Takeaways From 9th Circ. Facebook Case," for example). The most important thing businesses can do to avoid privacy-based claims is accurately disclose their privacy practices including, specifically, relating to the use of collection technologies such as cookies, pixels, and software development kits (SDKs). Drafting accurate privacy disclosures and implementing "just-in-time" notices (such as those required by the CCPA) will be the best way to defeat privacy-based claims.

5. Failing to Test Incident Response Plans.

Almost all data breach class action lawsuits include allegations relating to a business's failure to notify consumers of a data breach in a timely manner. To prevent this from being true, businesses should implement and test their incident response plans to ensure that their response to any security incident is quick and efficient. Indeed, the saying continues to be true – businesses are no longer being judged on whether a security incident occurs. Rather, the focus is on how they respond to the incident – with timing being a key component. Furthermore, if a business were to handle the incident response function properly, it may be able to "cure" the breach and avoid statutory damages afforded under the CCPA. For additional information, see our Bloomberg Law, "INSIGHT: First CCPA-Related Case Foreshadows Five Issues."

6. Failing to Consider What "Reasonable Security Procedures" Requires.

When establishing policies and procedures relating to information security, businesses would be doing themselves a disfavor if they did not consider what the phrase "reasonable security procedures" requires, especially in light of the CCPA's new statutory damages relating to data breaches. Although "reasonable security procedures" is left undefined as what is "reasonable" depends on the size of each business and the nature of the data each collects, the California Attorney General issued a report in 2016 providing its view that the Center for Information Security Top 20 Critical Security Controls ("CIS Controls") represents "the minimum level of information security that all organizations that collect or maintain personal information should meet." The report further provides that "[t]he failure to implement all the [CIS] Controls that apply to an organization's environment constitutes a lack of reasonable security." Id. In other words, the CIS Controls represent the baseline for "reasonable security procedures and practices," as required by Cal. Civ. Code § 1798.81.5. More information about the CIS Controls can be found by visiting this site: https://www.cisecurity.org/controls/cis-controls-list/.