Published on *The National Law Review* https://natlawreview.com

Litigation Minute: Mitigating Class Action Risks Posed by Collecting and Storing Sensitive Data

Article By:

Litigation at KL Gates

WHAT YOU NEED TO KNOW IN A MINUTE OR LESS

The collection and storage of sensitive data can not only invite the attention of government agencies, but also that of putative class action plaintiffs. Government inquiries, required disclosures, and media attention regarding alleged violations of data privacy law or data security incidents can—and often do—lead to the filing of follow-on class action litigation, which can easily compound the costs associated with such allegations and incidents.

In a minute or less, here is what you need to know about mitigating the risk of such class action lawsuits.

Keeping Up-to-Date Privacy Policies

Class action lawsuits relating to the collection and storage of sensitive data may involve statutory claims under federal and state consumer protection laws or common contractual or fraud claims. However, in many instances, the allegations focus not on practices regarding sensitive data, necessarily, but on the nature and extent to which such practices were sufficiently disclosed. Accordingly, one of the best ways to avoid potentially costly litigation is to regularly review and update applicable privacy policies.

More specifically, an entity that collects and stores sensitive data should update its privacy policies not only as required by evolving internal practices around sensitive data, but also to reflect trends in data privacy regulation and litigation. For instance, an entity may consider keeping an eye on enforcement actions and lawsuits against similar entities as a reference in determining best practices for disclosing relevant practices. Importantly, a robust privacy policy will reflect the increased level of protection afforded to certain classes of information, such as health information or personally-identifiable information, as well as reflect trends in what regulators and courts consider to constitute such information, which is constantly evolving.

Screening Third-Party Service Providers

Equally important is understanding the practices and policies of third-party service providers. It is rare

that an entity that collects and stores sensitive data does not employ the services of some third party. For instance, when developing software or online platforms, developers will often rely on third-party software development kits (SDKs) to streamline the development process and incorporate certain prepackaged features. Utilizing such SDKs has many benefits—for instance, allowing easy integration with social media, analytics, and other platforms without extensive coding?and is a highly common practice for many digital platforms.

However, in most cases, in order to achieve the sought-after functionality, some user information may need to be shared with the third-party SDK provider. Accordingly, an entity that follows even the most conservative data privacy practices may find itself subject to enforcement actions and follow-up class action litigation, whether founded or unfounded, on the basis of the use of a particular SDK. Screening any third-party service providers will go a long way to protecting any entity that partners with such providers.

Managing Data Security Incidents and Government Inquiries

Finally, being prepared to handle any data security incident or government agency inquiry quickly and carefully will further mitigate the risk of follow-up class action litigation. Nothing inspires putative class action plaintiffs more than a controversy, so the prompt and uneventful resolution of any such occasions is critical.

National Law Review, Volume XII, Number 144