Securities Law News

INSIGHT: First CCPA-Related Case Foreshadows Five Issues

By Ron Raether, Sadia Mirza, Oscar Figueroa, and Mary Kate Kamka
Feb. 10, 2020, 1:00 AM

The first lawsuit to cite to the California Consumer Privacy Protection Act is unlikely to test the law's limits, but should serve as a call for businesses to be ready, write Troutman Sanders attorneys. They offer five steps for preparing for more lawsuits.

On Feb. 3, plaintiff Bernadette Barnes filed a class action lawsuit hoping to be the first case to rely on the new California Consumer Privacy Act (CCPA). The complaint was filed over a data breach that allegedly occurred before the CCPA's Jan. 1, 2020, effective date.

Given this timing, this case will not test the limits of the CCPA; it is a false alarm.

However, the complaint foreshadows how plaintiffs are likely to rely on the CCPA and what steps businesses should take to be prepared.

The Allegations

Barnes alleges that hackers infected Hanna Andersson's e-commerce platform, operated by Salesforce.com, with malware that compromised customers' names and credit card information. The plaintiff claims that both defendants lacked reasonable procedures to protect customers' personal information, pursuing claims for negligence, declaratory relief, and a violation of California's Unfair Competition Law.

The lawsuit do not expressly bring a claim under the CCPA. Instead, it claims unspecified CCPA rights and alleges that the issue of whether the defendants violated the CCPA by failing to maintain "reasonable security procedures" is a common class issue.

1. The CCPA Does Not Provide the Unspecified Rights Claimed

Barnes claims that she, and the putative class members, were deprived of their rights under the CCPA. There are two notable issues here.

First, the CCPA does not afford consumers rights in the data breach context. Rather, consumers can recover statutory damages for a breach, but only if certain steps are followed. Thus, what "rights" the plaintiff has been deprived of remains unclear.

Second, the CCPA did not go into effect until Jan. 1, 2020. The CCPA does not expressly permit retroactive application required by California law.

2. The CCPA Does Not Create a Duty to Maintain Reasonable Security Procedures

The CCPA imposes no obligation on businesses to maintain reasonable security procedures. Rather, the CCPA provides that, under certain circumstances, consumers may be entitled to statutory damages in the event of a data breach.

Nonetheless, this case serves as an important reminder for businesses to evaluate their security environments against the Top 20 Critical Security Controls (CIS Controls), which the California attorney general recognizes as representing the "minimum level of information security that all organizations that collect or maintain personal information should meet."

The AG further stated that the "failure to implement all the [c]ontrols that apply to an organization's environment constitutes a lack of reasonable security."

3. The CCPA's Cure Provision May Give Businesses an Out

The CCPA allows consumers to bring an action for statutory damages in the event of a data breach due to a business's failure to implement reasonable security procedures. However, prior to bringing an action, the consumer must provide the business a 30 days' written notice identifying the specific violation. If the business cures the noticed violation and provides the consumer a written statement indicating such, statutory damages are not available.

What qualifies as a cure remains unclear, but businesses should give careful thought to their breach notice as well as the written response.

On one hand, if a business believes that reasonable security procedures are intact, the business's breach notice, written response, and actions should communicate this message consistently. The value of an incident response plan tested through tabletop exercises cannot be overstated. Indeed, if a business were to handle the incident response function properly, curing the noticed violation may prove easy. Statements concerning the health of the business's security environment in a breach notice or any changes to existing security procedures in the event of a breach will be a doubled-edged sword, so businesses should take caution.

On the other hand, if a business believes that heightened data security procedures are warranted, businesses may be able to cure the alleged deficiency by implementing practices promoted by guideline documents adopted to aid in the area of information security (*e.g.*, NIST Cybersecurity Framework or the CIS Controls), or the data security practices promoted or sometimes mandated by the FTC. Choosing this path, however, may destroy any argument that the business maintained reasonable security procedures.

4. CCPA's Statutory Damages for Data Breaches Do Not Apply to 'Service Providers'

The CCPA draws a distinction between entities acting as "business[es]" and entities acting as "service provider[s]." A service provider is generally an entity that processes personal information on behalf of a business pursuant to a written contract that includes the required language.

Notably, only "businesses" that fail to implement reasonable security procedures may be held liable for the statutory damages. For this reason alone, all entities that process personal information on behalf of a regulated business should assess whether it meets the definition of "service provider" and, if so, update its contracts accordingly.

The contract should clarify that there are no third-party beneficiaries to the agreement, no special relationships and, specifically, no duty to consumers. From the businesses' perspective, the contract should require service providers to coordinate in the event of an incident, which may help avoid the many issues.

5. Obligation to Maintain Reasonable Security Procedures Only Applies to Businesses that 'Own,' 'License,' or 'Maintain' Personal Information

California law only requires entities to maintain reasonable security procedures to the extent that they own, license, or maintain personal information. If an entity does not engage in the foregoing activities, it is arguably under no obligation to maintain reasonable security procedures. Without such obligation, the entity cannot be liable for the CCPA statutory damages.

For businesses that provide customers with software-as-a-service solutions, which are generally not designed to maintain or store data, clarifying this point in contracts and marketing materials could help to avoid unnecessary litigation.

Indeed, if it were obvious to consumers that an entity does not collect or store personal information, a vendor, like Salesforce, may not have been pulled into the complaint in the first instance.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

Ron Raether leads the Cybersecurity, Information Governance and Privacy practice group at Troutman Sanders LLP, and is a partner in the firm's Financial Services Litigation group. He is known as the interpreter between businesses and information technology, and has assisted companies in navigating federal and state privacy laws for over 20 years, defending hundreds of putative class actions making privacy-based claims.

Sadia Mirza, an attorney at Troutman Sanders LLP, focuses her practice on cybersecurity and privacy issues and compliance across the financial services industry. She is a knowledgeable transactional counsel with experience in-house, positioning her to interact effectively with business, compliance, legal and information security departments.

Oscar Figueroa is an attorney in Troutman Sanders' Orange County office who focuses his practice on intellectual property and business litigation matters. He has litigation experience in California state court and federal courts throughout the country.

Mary Kate Kamka, an attorney in Troutman Sanders' Consumer Financial Services Practice, is an experienced litigator in both individual cases and complex class actions from the outset of a case through trial. She focuses on consumer and commercial financial services litigation specializing in both class action and individual cases.

TOP

MORE INFORMATION

About Us
Contact Us

Securities Law News

Terms of Service
Copyright
Privacy Policy
Accessibility