Court Confirms Kentucky Consumer Protection Act Doesn't Cover Employees, But Legal Risks Remain: 5 Steps for Employers to Avoid Data Breach Lawsuits

Insights
5.15.25

A federal district court recently found that employees aren't protected by Kentucky's consumer protection law because they don't qualify as consumers, handing a solid win to employers. The April 21 decision in *Viviali v. One Point HR Solutions, LLC* saw the court dismiss a Kentucky Consumer Protection Act (KCPA) claim brought by a former employee whose personal data was stolen by cybercriminals. However, the court permitted KCPA claims brought by customers who also had their data stolen to proceed – in part because of the company's delay in informing customers about the breach – as well as all other legal claims brought by the customers and the employee alike. This ongoing court battle demonstrates why companies not only need to continuously monitor their technology systems for any breaches, but promptly inform their consumers – and employees – if a breach does occur. What do you need to know about this case and what five steps should you take to best position your organization?

What Triggers a Violation of the KCPA and Who Enforces It?

The KCPA was enacted to provide consumers broad protections from illegal acts.

- It protects Kentucky's citizens from "unfair, false, misleading, or deceptive acts or practices in trade or commerce."
- KCPA applies to "any person who purchases or leases goods or services primarily for personal, family or household purposes and thereby suffers any ascertainable loss of money or property, real or personal, as a result of the use or employment by another person of a method, act or practice declared unlawful by KRS 367.170."
- To establish a KCPA claim, a plaintiff must prove that the defendant engaged in unlawful acts or practices, that the plaintiff is a consumer that purchased goods or services for personal, family, or household purposes, that the plaintiff suffered an ascertainable loss, and that plaintiff's damages are the natural and probable consequence of the defendant's conduct.
- In addition to individual consumer actions, the Kentucky Attorney General's Office of Consumer Protection also enforces the KCPA. The Office of Consumer Protection enforces the KCPA by bringing lawsuits in the public interest to obtain civil penalties and consumer redress, including restitution and injunctive relief aimed at changing bad business practices.

What Happened?

One Point is an outsourcing company that helps organizations automate and manage human resources operations. Cybercriminals initiated an attack on One Point's network in July 2023 and gained access to PII such as social security numbers, driver's license numbers, passport numbers, health insurance information, and credit card information. The breach spanned from July 3, 2023, to February 14, 2024 – but One Point did not notify victims of the breach until September 24, 2024.

Plaintiffs Charles Viviali, Lisa Alecia, and Kayla Lofton alleged that One Point failed to implement reasonable and adequate data security measures and to provide timely notice of the breach. They all brought a variety of legal claims against One Point, including violations of the KCPA. Notably, Viviali was a former employee of One Point, while the other two plaintiffs were simply customers.

Employee's KCPA Claim Dismissed

The court found that Viviali could not be considered a consumer under the definition of the KCPA since he was an employee of One Point. It cited a 2022 federal court case to support this ruling and noted that Viviali presented no contrary case law to support a KCPA claim brought against an employer. Therefore, it dismissed his KCPA claim.

Customers' KCPA Claims Given the Green Light

However, the court permitted the other two plaintiffs to proceed with their KCPA claims. One Point argued that it shouldn't be subject to the state consumer protection statute because it wasn't engaged in trade or commerce, as it primarily deals in human resources operations. However, the court found that, given One Point's delayed breach notification, the other two plaintiffs had plausibly alleged that they had potentially purchased services from One Point as consumers and that the KCPA applied.

Mixed Outcome for Other Claims

- The court dismissed several of the other claims, including negligence per se, breach of confidence, breach of the implied covenant of good faith and fair dealing, breach of fiduciary duty, and requests for declaratory and injunctive relief.
- However, the court allowed claims for negligence, breach of implied contract, unjust enrichment, and invasion of privacy to proceed.
- Though Viviali, the former employee of One Point, was not considered a consumer under the KCPA, the court allowed his claims of negligence, breach of implied contract, unjust enrichment, and invasion of privacy to proceed. This serves as a good reminder to employers to protect employee PII to the best of their ability and promptly inform them of any cybersecurity breach.

Your Next 5 Steps

Here are five steps you can take to minimize the chances of facing liability for a data breach claim.

1. **Familiarize Yourself with Applicable Law**
   Ensure you, as well as your employees, have a thorough understanding of what constitutes PII. You should also ensure that you are familiar with what constitutes a breach under the KCPA and other applicable laws. This includes when the disclosure of certain types of data constitutes a data breach. Seek legal advice from your privacy counsel on your obligations and potential risks regarding what kind of data you store about both your consumers and employees.
2. **Monitor For Breaches Frequently**
   Monitor for any potential data breaches. If one occurs, take immediate action to secure the network and change network access authorization to prevent the breach from getting worse.
3. **Contact Privacy Counsel Regarding a Breach**
   Legal counsel can help you analyze and comply with data breach notification and other reporting obligations resulting from the breach. They can also help you supervise and direct outside vendors conducting investigation of the breach. Having counsel direct vendors may create privilege in the communications regarding the investigation, which could be useful if the breach results in litigation.
4. **Contact Your Service Provider**
   If a service provider is responsible for the breach (such as your web security company, website builder, third-party payment processor, or similar companies), review any applicable agreements to determine the obligations of the parties. If appropriate, ensure that the provider is investigating, remedying, and responding to the breach. You should also reassess their access privileges and verify that vulnerabilities were indeed remedied by the provider.
5. **Stay on Top of Changes**
   State and federal consumer protection and privacy laws are constantly changing and being interpreted and applied in new ways. Staying up to date on developments will help you remain compliant with obligations under the KCPA, the Kentucky Consumer Data Protection Act (KCDPA) – which takes effect January 1, 2026 – and other applicable state and federal laws.

Conclusion

As technology evolves, so do the methods used by cybercriminals. Failing to act swiftly after a breach can result in costly litigation under various state laws, including the KCPA. Organizations must proactively refine their data security and privacy practices and contact privacy counsel immediately in the event of a breach to ensure legal compliance and minimize liability.

If you have any questions about best practices for addressing data breach threats, please consult your Fisher Phillips attorney, the author of this Insight, any attorney in our Louisville office, or a member of our Privacy and Cyber Practice Group or our Data Protection and Cybersecurity Team. To ensure you stay up to speed with the latest developments, make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.

Related People

Annie N. Harb
Associate
502.561.3984
Email

Service Focus

Consumer Privacy Team

Data Protection and Cybersecurity

Litigation and Trials

Privacy and Cyber

Trending

U.S. Privacy Hub

Related Offices

Louisville