alert Cybersecurity and Privacy Practice

Saul Ewing LLP

JULY 2017

NJ Seeks to Protect Consumer Data with Personal Information Privacy and Protection Act

Author:
Francis X. Riley III

SUMMARY

A recently enacted New Jersey law restricts retailers from collecting and using personal information gleaned from driver's licenses and other identification cards. The law, which will take effect October 1, 2017, is meant to crack down on the risk of data breaches and the sale of consumer information to marketers.

Under the Personal Information Privacy and Protection Act, retailers can only scan customers' identification cards for certain purposes, including to verify the authenticity of the card or a consumer's identity or age, and the information that they can collect from these scans is limited to the person's name, address, date of birth, the state the identification card was issued in, and the identification card number. Additionally, the law requires retailers to securely store this data and report any security breaches in accordance with the state's notification law, and prohibits them from sharing the information with marketers or other third parties that are unknown to consumers.

Retailers are still able to scan shoppers' identification to verify their identity if the shopper is not paying with cash, or if they return an item or request a refund or exchange. They can also do so to verify consumers' age when they're purchasing age-restricted goods or services or in an attempt to prevent fraud or other criminal activity in the case of a merchandise return or exchange or in the context of a credit transaction to open or manage a credit account. Retailers can also scan IDs to record, retain or transmit information as required by state or federal law; to transmit information to a consumer reporting agency, financial institution or debt collector pursuant to laws such as the Fair Credit Reporting Act, Gramm-Leach Bliley Act, and the Fair Debt Collection Practices Act; to establish or maintain a contractual relationship; and to record, retain or transmit information by a covered entity governed by medical privacy and security rules. However, businesses cannot retain information related to how the person paid for the goods, if they returned an item or if they requested a refund, and they cannot store ages if an ID is scanned when purchasing an age-restricted item. Additionally, the limited information that retailers are allowed to retain from these scans must be "securely stored," and any security breach of the information must be reported to any affected person and the New Jersey State Police.

Violation of the new law carries civil penalties of $2,500 for a first offense and $5,000 for any subsequent misstep. The Act allows for "any person aggrieved by a violation" to bring an action in Superior Court to recover damages.

The Cybersecurity and Privacy attorneys at Saul Ewing LLP regularly counsel clients with regulatory, compliance, and litigation concerns associated with cybersecurity. For more information on this alert, please contact the author or the attorney in the firm with whom you are regularly in contact.

This Alert was written by Francis X. Riley III, Co-Chair of the firm's Consumer Financial Services Practice. Francis can be reached at 609.452.3150 or friley@saul.com. This publication has been prepared by the Cybersecurity and Privacy Practice for information purposes only.