Client Alert: New Jersey Enacts Restrictions on Retailers' Collection and Use of Consumer Identification Information

Related Professionals

Marcel C. Duhamel

Natalia Steele

Related Services

Litigation and Appeals

CLIENT ALERT | 7.27.2017

On July 21, New Jersey Governor Chris Christie signed the "Personal Information and Privacy Protection Act." The new law, effective October 1, 2017, imposes restrictions on when a "retail establishment" can scan information from a consumer's driver's license or state-issued identification card, and on what the retailer may do with that information once it has it. The statute will present compliance challenges, particularly for retailers conducting business in multiple states.

On its face the statute governs only information obtained from a "scan" of a card. "Scan" is defined as "to access the barcode or any other machine readable section of a person's identification card with an electronic device capable of deciphering, in an electronically readable format, information electronically encoded on the information card." The statute does not speak to when or whether a retailer may capture the same information manually. Retailers are permitted to scan a card only for eight specific reasons:

1. to verify the card's authenticity or to verify the person's identity if the person is paying for goods and services with a method other than cash, returns an item, or requests a refund or exchange;
2. to verify a person's age, if the retailer is providing age-restricted goods or services to the person;
3. to prevent fraud "or other criminal activity" if the person is returning an item or requesting a refund or exchange and the retailer uses a fraud prevention service company or system;
4. to prevent fraud "or other criminal activity" related to a credit transaction to open or manage a credit account;
5. to establish or maintain a contractual relationship;
6. to record, retain, or transmit information as required by State or federal law;
7. to transmit information to a consumer reporting agency, financial institution, or debt collector to be used as permitted by the Fair Credit Reporting Act, the Gramm-Leach-Bliley-Act, and the Fair

Debt Collection Practices Act; and

8. to record, retain, or transmit information by a covered entity governed by the medical and security rules promulgated under the Health Insurance Portability and Accountability Act.

Even when a scan is permitted, the retailer is permitted to capture only certain information: the person's name, address, and date of birth, the state issuing the identification card and the identification card number.

Retailers are not permitted to "retain" information obtained for reasons numbered 1 and 2 above. The statute does not purport to define precisely how long a retailer can keep that information before it is deemed to have "retained" it. Information obtained for the remaining reasons must be "securely stored," and any breach of that security must be "promptly reported" to the state police and to the affected persons. Neither "securely stored" nor "promptly reported" are defined terms.

The statute expressly prohibits selling or disseminating any information to third parties, including marketing, advertising, or promotional activities, except as permitted by reasons three through eight for collecting the information.

The statute creates a private right of action for damages. It also provides a civil penalty of $2,500 for a first violation and $5,000 for any subsequent violation.

A few specific compliance challenges present themselves immediately. The statute's ambiguity with respect to what constitutes "retaining" information may create confusion; must a retailer avoid recording information viewed from a scan in order to ensure compliance? If the information is recorded, must it be deleted immediately? If the information is captured by a back-up system, must it be immediately purged from that system? Will retailers be able to reconfigure already existing software and systems to comply with both the restriction against retention under some circumstances but not others, and with the limit on information it is permissible to collect?

Perhaps, though, the greatest compliance challenge will be faced by retailers doing business in multiple states as states adopt competing and conflicting requirements. Several other states have also enacted restrictions on scanning consumer IDs or on using information obtained from those scans. Ensuring compliance with all of those requirements may add complexity to an already complicated landscape.