New Jersey Amps Up Focus on Privacy and Cybersecurity

Alysa Z. Hutnik, Glenn T. Graham

November 18, 2019

California is not the only state focused on privacy. The New Jersey Attorney General's Office recently emphasized how the Office is prioritizing its enforcement of such issues. Over its first year, the newly-created Data Privacy & Cybersecurity Section within the New Jersey Division of Law has initiated its own actions and joined several multi-state investigations. Privacy also plays a prominent role in private actions and draft legislation in the Garden State. Companies marketing or selling to New Jersey consumers or otherwise operating in the state should take steps to confirm their privacy compliance.

Reported Data Breaches

According to statistics released by the New Jersey Attorney General and Division of Consumer Affairs on October 31, 2019, there were 906 separate data breaches reported to the New Jersey State Police in 2018, compared to 958 breaches in 2017. The number of individual residents impacted declined significantly from 2017 to 2018. While over 4 million residents were impacted by 2017 breaches, that number fell to approximately 358,000 in 2018. The 2018 total, however, is still nearly three-times the 116,000 residents impacted in 2016.

State Enforcement Actions

In response to these breach figures, New Jersey actively enforced against lax privacy practices. Through the first three quarters of 2019, the Attorney General reported $6.4 million in recoveries. Additionally, New Jersey served a leading role in several large-scale, multi-state recoveries for consumers over the last 9 months. For example:

- New Jersey was part of the Leadership Committee pushing the investigation and resolution of claims arising from a 2017 data breach at credit reporting agency Equifax that will result in payment of $575 to $700 million ($6.36 to NJ) as part of a global resolution of claims by the FTC, 50 U.S. states and territories, and individual consumers.
- New Jersey was also one of 30 states to resolve data breach and consumer privacy claims against health insurer Premera Blue Cross Blue Shield. Premera's network had exposed the Social Security and sensitive health information of 10.4 million consumers, including approximately 40,000 NJ residents. That settlement includes $10 million to the states (including $72,168 to NJ) as well as a $32 million fund for consumers and $42 million in required cybersecurity upgrades at Premera.
- New Jersey was also part of the multi-state resolution of claims against retailer Neiman Marcus in response to a breach involving shoppers' credit card numbers and other personal information. NJ received $57,465 as part of a $1.5 million settlement, which impacted

approximately 17,000 individuals with NJ addresses.

Private Consumer Actions

The millions of New Jersey residents impacted by data breaches and cybersecurity threats over the last several years has served as a large pool of potential private litigants. The New Jersey courts remain an active destination for putative consumer class actions arising from data security and privacy issues. In addition to recovery for losses, New Jersey's Consumer Fraud Act includes provisions that can allow for treble damages as well as awards for all costs and attorney fees. Such provisions make privacy and data breach issues a ripe target for private consumer claims.

Similarly, the District of New Jersey has handled a number of complex privacy matters, including the recently-formed Multi-District Litigation arising from a data breach at American Medical Collection Agency Inc. that implicates patient data from approximately 20 million people related to Quest Diagnostics and LabCorp.

Legislative Focus on Privacy

Following the national trend, New Jersey's lawmakers have shown a consistent interest in increased regulation of data privacy and cybersecurity. There are at least 18 separate bills currently pending in the Legislature that address privacy and cybersecurity. That includes both Senate and Assembly legislation that would require development and implementation of a "comprehensive information security program" by businesses that handle personal information. In May, Governor Murphy signed a bill expanding the definition of personal information to include online account information as part of the State's data breach notification law.

With the increased public awareness of comprehensive privacy and cyber legislation garnered by the EU's GDPR and California's CCPA, businesses should be prepared for other states to follow suit. Given its prior history as a leader on consumer-focused legislation, companies can expect New Jersey legislators to seriously consider additional privacy legislation.

New Jersey is only one example of how consumer privacy issues are being addressed at the state level. Harmonizing business practices across state lines may prove challenging as these new laws regulating data practices are enacted. For now, as a best practice, it's helpful to:

- Take steps to keep privacy and cybersecurity practices, policies, and procedures in line with each state where your customers reside;
- Determine if your compliance program takes into account and reasonably addresses foreseeable risks to the personal information in your control, and whether this risk analysis is documented so you can point to it if needed if there's a future lawsuit or government investigation;
- Evaluate whether the business has sufficiently invested in adequate privacy and cybersecurity and insurance coverage that takes into account how the business, laws, and potential exposure are evolving; and
- Consult with experienced practitioners in this area that can help guide and counsel your business on options for making practical updates to your compliance program mindful of the changing legal landscape.