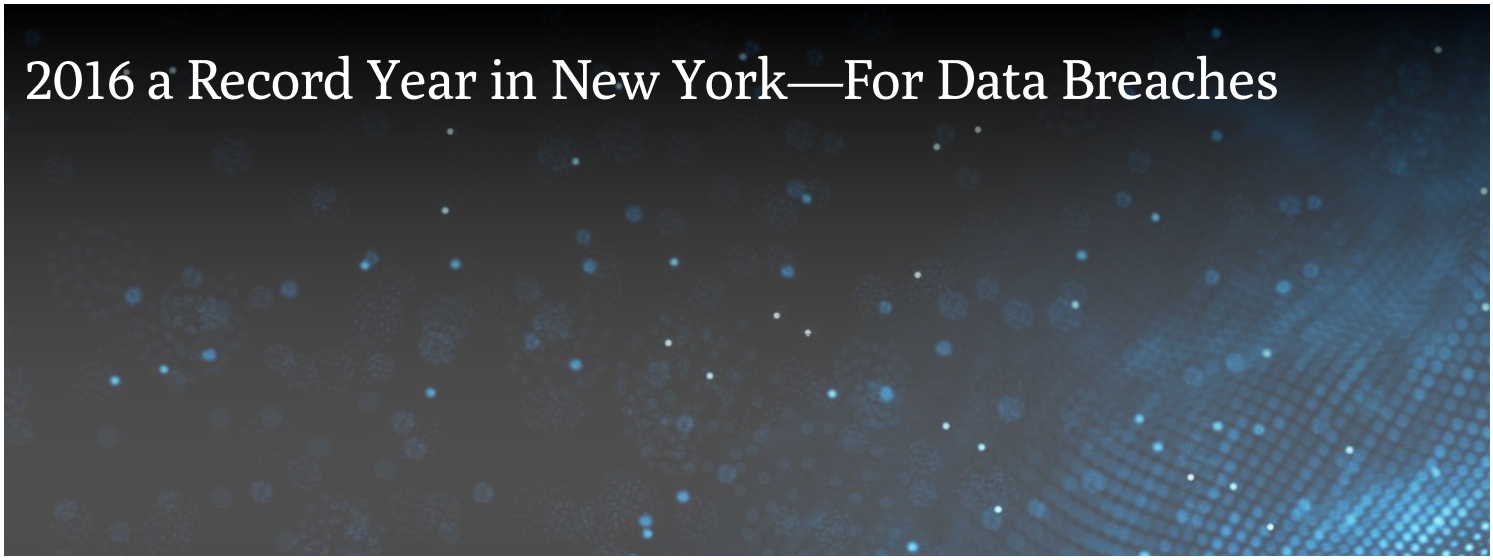
WINSTON & STRAWN LLP

BLOG

# 2016 a Record Year in New York—For Data Breaches



MARCH 27, 2017

New York Attorney General Eric Schneiderman recently announced that his office received a record number of data breach notices in 2016. Nearly 1,300 breaches were reported, impacting over 1.6 million New Yorkers. These figures represent a 60% increase in the number of reported breaches from 2015, and a three-fold increase in the number impacted individuals. Two noteworthy trends emerged from the data released by AG Schneiderman's office. First, while hacking remained the leading cause of data breaches in New York last year (40%), employee-related causes came in a close second (37%). Specifically, inadvertent exposure of records (e.g., an HR employee falling for a phishing scam), insider wrongdoing (e.g., a disgruntled employee), and the loss of a device or laptop collectively accounted for more than a third of breaches in the state last year. This suggests that employers, in addition to continually focusing on hardening their protections against external threats, may also want to consider new ways to reduce the prevalence of employee-caused data breaches. The second noteworthy data trend relates to the categories of information most frequently targeted. Social Security Numbers accounted for nearly half of all compromised records (46%). Financial account information accounted for a third of compromised records (35%). The next closest type of information targeted was financial account information (8%).

The Attorney General's office offered several suggestions to organizations to help reduce the threat of a breach. First, understand where your business stands. What information does your business requires for its operation? What data has your organization collected and stored, and how long do you keep the data? How is information shared with third parties, and what access controls are in place? Second, minimize data collection practices. Collect only information that is needed, and keep it only for as long as you need it. Third, create and execute an information security plan. Fourth, take immediate action in the event of a breach. Investigate all security incidents immediately, and in the event of a breach, keep track of the various legal requirements that may be triggered based on the circumstances.

**TIP: Companies should take heed of Attorney General Schneiderman's recommendations for reducing the threat of a breach and also consider the importance of involving legal counsel in a breach response to provide experience, expertise, and preserve privilege.**

2 Min Read

## Related Locations

Chicago

New York

## Related Topics

Data Breach

## Related Capabilities

Privacy & Data Security

## Related Regions

North America

*This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.*