MorrisonCohen LLP

Law Firm to the Middle Market®

New York Legislature Tightens Data Security Duties; Broadens Reach; Expands Penalties

July 2, 2019 – Under a bill enacted in the closing days of the Albany legislative session last month, all businesses having personal and private data concerning New York residents will be required to adopt formal data security practices and procedures tailored to the risks and size of their business or face administrative injunctions and substantial fines and penalties.

The so-called "SHIELD Act," drafted as a consumer protection measure at the request of the Office of the Attorney General, and now awaiting the Governor's signature, addresses three principal issues: 1) the types of information that must be protected from breach; 2) the obligations a business must adopt to prevent a breach and to provide notice if a breach occurs; and 3) the scope of what a breach of security actually means.

The bill would expand the existing types of covered information subject to protection under the Act to include electronic records of a person's biometric data (such as a fingerprint or retinal scan), and a person's email address if accompanied by access credentials (such as a password or security questions), and would apply to all businesses, wherever located, rather than only businesses located within the state of New York.

Affected businesses are divided into two basic groups. Those that already must comply with existing data security regulations, such as financial institutions and health care providers are largely unaffected by the bill, with the exception of having a few additional notice requirements in the event of a security breach. Everyone else having private data about New Yorkers, however, will need to meet its compliance scheme.

Other than entities that qualify as a "small business," which is defined by number of employees, annual revenue or year-end assets, and whose compliance burden is somewhat less comprehensive, businesses will effectively be required to adopt, maintain and keep updated a security regime meeting, at a minimum, fairly specific risk-adjusted administrative and technical safeguards, including training and supervision of information security personnel, and regular testing of the adequacy of the businesses' data security infrastructure.

Perhaps most importantly, businesses that engage third parties to maintain and process their data, as all those who store data on the cloud do, will have to ensure that their service providers are contractually bound to provide them the same appropriate risk-adjusted level of data security. This will likely entail a need by all businesses to re-examine the nature of their cloud service, web hosting, and ecommerce agreements to ensure appropriate coverage, since many such agreements do not presently incorporate such a requirement.

The bill also expands the concept of a breach by including any type of unauthorized data access (including by insider personnel), rather than the actual acquisition of the data by third parties, as under current law.

The bill is expected to be presented to the Governor for signature shortly, and would become law immediately.

For additional information concerning current data privacy and security laws and regulations, please contact your regular Morrison Cohen lawyer.