Protection of Employee Private Information

In an effort to further protect the personal information of its residents, New York State recently enacted the Stop Hacks and Improve Electronic Data Security Act (the "SHIELD" Act), which applies to employers that maintain information about New York-based applicants and employees. This law is applicable to all such employers, whether they are located inside or outside of New York, and regardless of size. As set forth below, employers must be acutely aware of the information they collect from employees, how it is safeguarded, how long it is kept, and how to respond in the event of a data breach.

Reasonable Safeguards

The SHIELD Act requires any person or business that owns private information[1] of a resident of New York to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information" as of March 21, 2020. Employers will satisfy this standard if they implement a data security program that includes:

- Reasonable administrative safeguards, such as the following: (a) the designation of one or more employees to coordinate the security program; (b) identification of reasonably foreseeable internal and external risks; (c) assessment of the sufficiency of the safeguards in place to control the identified risks; (d) training and managing employees in the security program practices and procedures; (e) the selection of service providers capable of maintaining appropriate safeguards and requiring that those safeguards are maintained by contract; and (f) adjusting the security program in light of business changes or new circumstances.

- Reasonable technical safeguards, such as where the employer: (a) assesses risks in network and software design; (b) assesses risks in information processing, transmission, and storage; (c) detects, prevents and responds to attacks or system failures; and (d) regularly tests and monitors the effectiveness of key controls, systems and procedures.

- Reasonable physical safeguards, such as where the employer: (a) assesses risks of information storage and disposal; (b) detects, prevents, and responds to intrusions; (c) protects against unauthorized access to or use of an employee's private information during or after the collection, transportation, and destruction or disposal of this information; and (d) disposes of an employee's private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.

[1] Private information includes any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person in combination with any one of the following: (i) social security number; (ii) driver's license number or non-driver identification card number; (iii) account number, credit or debit card number, in combination with a security code, access code, password or other information that would permit access to an individual's financial account; (iv) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or (v) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity.

An employer that is a small business under the Shield Act (*i.e.*, that has fewer than 50 employees, generated less than three million dollars in gross annual revenue in each of the past three fiscal years, or has less than five million dollars in year-end total assets) will be considered in compliance with the Act if they have a security program that contains reasonable administrative, technical, and physical safeguards that are appropriate for the size and complexity of the employer, the nature and scope of the employer's activities, and the sensitivity of the personal information the employer collects from or about its employees.

In the Event of a Breach

While employers are not required to implement the reasonable safeguards described above until March 21, 2020, the Shield Act currently imposes new notification requirements in the event of a breach of private information. If there is unauthorized access (*i.e.*, viewing) or acquisition of private information, the employer must expediently disclose the breach to any employee whose private information was, or is reasonably believed to have been, accessed or acquired without valid authorization. Such notice is not required, however, if the exposure of employees' private information was an inadvertent disclosure by persons authorized to access their private information and the employer reasonably determines that such exposure will not likely result in misuse of such information, financial harm to the affected employees, or emotional harm in the case of unknown disclosure of online credentials. If the unauthorized disclosure affects over 500 New York employees, the employer must provide such a determination in writing to the State Attorney General within 10 days after the determination is made.

If an employer is required to provide such a notification to its employees, the employer must notify the State Attorney General, the Department of State, and the Division of State Police as to the timing, content, and distribution of the notice and the approximate number of affected employees, and the employer must also provide a copy of the template of the notice that was sent to the affected employees. In the event that more than 5,000 New York employees are to be notified at one time, the employer shall also notify consumer reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected employees.