A NEW ILLINOIS LAW IMPOSES NOTIFICATION REQUIREMENTS ON BUSINESSES THAT MAINTAIN PERSONAL INFORMATION

Information security is an emerging liability issue for nearly every business in the world, especially those operating in the United States. Thirty-nine states, including Illinois, have enacted laws that impose duties on businesses if the integrity, security or confidentiality of certain types of information maintained by the businesses is comprised. The Illinois Personal Information Protection Act ("Act'), 815 ILCS 530/1 et seq., as amended by P.A. 94-947, mandates that any "data collector" that owns or licenses "personal information" on an individual must notify that person at no charge when there has been a "breach of the security of the system data" or written material following discovery or notification of the breach. Failure to comply with the Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act, which provides for the potential imposition of punitive damages against the business.

Irrespective of size, type or industry, virtually every business is a "data collector" and consequently subject to the Act. The definition of "data collector" expressly includes, among others, private corporations and retail operators as well as "any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information."

The Act defines "personal information" as an individual's first name or first initial and last name in combination with any one or more of the following data elements:

a. Social Security number;
b. Driver's license number or State identification card number;
c. Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Law firms, accounting firms, health care providers, financial and educational institutions, and insurance companies undoubtedly maintain "personal information." Most businesses maintain employee personnel files and payroll data that contain "personal information." Many businesses maintain sales records, customer lists and prospect lists which may contain "personal information." The "personal information" may belong to employees, independent contractors, customers, clients, prospects, patients, students, vendors or any other individual.

The duty to notify is triggered when there is a "breach of the security of the system data," which is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. This does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector.

In other words, if an unauthorized person obtains “personal information” from a "data collector" or if an authorized person obtains “personal information” to use for an improper purpose, then the Act requires the “data collector” from whom the “personal information” was taken to notify those individuals whose “personal information” was compromised.

Once the Act is triggered, the “data collector” must notify the individuals at no charge that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification must be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

The best way to deal with the requirements of the Act is to design and implement an information security program that will protect against the unauthorized disclosure of "personal information" as well as establish procedures to minimize liability and business disruption. Contact us today to discuss an information security program that will address your business' information security issues.