CSR®
Privacy Made Simple℠

State of Illinois

Statutory Review for Breach & Consumer Notification

This summary of regulations is provided for information purposes only. No action based on this summary alone should be undertaken. Each individual or entity must obtain appropriate guidance for its specific circumstances.

48 states and the District of Columbia (Washington DC) have laws pertaining to the way they expect a breach to be handled and how they want their affected residents to be notified. If you have customers or have personal information pertaining to individuals that reside outside of your state, you will additionally need to ensure that you follow the laws of that corresponding state or country.

Following is a brief review of the Illinois laws pertaining to breach and consumer notification.

Personal Information
There is specific personal information that the state considers relevant to a breach. (This does not include elements that a federal agency or industry specific entity may consider relevant.)
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. d) Medical Information; e) Health insurance information; f) Unique biometric data used by the owner or licensee to authenticate an individual, such as fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; g) User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security.

Who does the law apply to?
The state will identify who the law pertains to. The state may have different laws for state agencies or specialized fields such as medical or financial.
The law applies to any data collector that owns or licenses personal information concerning an Illinois resident. "Data collectors" are considered government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with non-public personal information. Additionally, if personal information is being maintained or stored by a third-party that does not own or license the data (vendor), and the vendor is breached, the vendor must immediately notify the data owner or licensee (data owner). The data owner is responsible to complete the reporting and consumer notification requirements. The vendor must additionally cooperate by supplying the date or approximate date of the breach, the nature of the breach, and informing the data owner of any steps they have taken or plan to take. The cooperation does not require disclosure of confidential business information or trade secrets.
Breach
There are many factors to take into consideration when deciding if the incident is considered a breach and when that breach is reportable. Some states have very specific factors while others leave the interpretation open to include a multitude of elements.
In Illinois, any unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information. When considering reporting requirements, it would additionally include, but not be limited to: • The combination of personal information breached; • If health insurance, medical and/or unique biometric data information were breached; • If the data was encrypted or redacted; • If the data included any kind of key or cipher. For Illinois state agencies, it also includes written material.
Breach Reporting
There may be specific time limits to report a breach and complete consumer notification. There may be specific entities to report to.
The notification may be delayed if law enforcement gives the data owner a written request to do so as the notification may interfere with an investigation.

Breach Reporting (cont'd)
Illinois also specifies notice to the attorney general in certain circumstances for businesses subject to Health Insurance Portability and Accountability Act (HIPAA) and/or Health Information Technology for Economic and Clinical Health Act (HITECH). There is a timeframe. State agencies must notify Attorney General within forty-five (45) days (or sooner), if more than 250 Illinois residents are affected and if more than 1,000 consumer notifications will be sent, they must also report it to the consumer reporting agencies.
Notifications
Notifications to the consumer may require detailed information and sometimes provision of services. The notifications must be sent or delivered in a specific manner.
Illinois has a wide-ranging list of detailed information to be included in the notification, including consumer reporting agency and FTC information. The notification may only be delivered by mail or sent electronically (consistent with US Code Section 7001 of Title 15) A substitute notice can be sent if the business (or State agency) demonstrates that the cost of providing the notice would exceed $250,000 or the persons to be notified exceeds 500,000, or they do not have sufficient contact information. Substitute notice must consist of ALL of the following: email notice, conspicuous posting on their website, and notification to statewide or local media.
Penalties for Non-Compliance or Violations
In almost all states, the state attorney general may bring action upon an entity that has not complied with their breach and/or consumer notification laws.
In Illinois, violation constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act. The Attorney General may investigate, require written statements or a report under oath, issue subpoenas, conduct hearings, and promulgate rules with the force of law. Remedies are available for preliminary or permanent injunctive relief; revocation of licenses; dissolution or suspension of corporations, restitution, civil penalties, and punitive damages.

CSR®
Privacy Made Simple℠

Applicable Laws
For more information, review your state statutes:
The statutes include, but are not limited to: Illinois Compiled Statutes: • Chapter 815 Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505 • Personal Information Protection Act, 815 ILCS 530/1 through 815 ILCS 530/50 All entities should ensure there are no additional statutes applicable to them due to their type of business or activity. In addition, entities should ensure they have complied with federal laws or industry regulations that may also apply. For entities with out-of-country personal data, laws in those countries should also be reviewed for applicability.
Other Related Laws
In order to ensure protection of personal information BEFORE a breach happens, many states now have laws for data protection, data retention, and/or data disposal.
Illinois requires businesses and agencies in their state to follow laws for disposal of materials containing personal information. Business Transactions Deceptive Practices / (815 ILCS) Personal Information Protection Act / Sec. 30 Safe disposal of information, Sec. 40 Disposal of materials containing personal information; Attorney General, Sec. 45 Data Security, and Sec. 50 Entities subject to federal HIPAA, 1996. Violating these laws can result in the state attorney general imposing a civil penalty of $100 per person whose personal information was not disposed of properly, but not higher than $50,000 per incident. All entities should ensure there are no additional statutes applicable to them due to their type of business or activity. In addition, entities should ensure they have complied with federal laws or industry regulations that may also apply. For entities with out-of-country personal data, laws in those countries should also be reviewed for applicability.