RÉSUMÉ DIGEST

ACT 382 (SB 361) **2018 Regular Session** **Walsworth**

Prior law defined "breach of security of the system" as the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information maintained by an agency or person.

New law defines "breach of the security system" as the compromise of the security, confidentiality, or integrity of computerized data that results in, or there is a reasonable likelihood to result in, the unauthorized acquisition of and access to personal information maintained by an agency or person.

Prior law defined "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, when the name or the data element is not encrypted or redacted:

(1) Social security number.

(2) Driver's license number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

New law defines "personal information" as the first name or first initial and last name of an individual resident of this state in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:

(1) Social security number.

(2) Driver's license number or state identification card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4) Passport number.

(5) Biometric data.

New law defines "biometric data" as data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account.

New law requires any person that conducts business in the state or owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

New law requires any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information to take all reasonable steps to destroy or arrange for the destruction of the records within its custody or control containing personal information that is no longer to be retained by the person or business by shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

Prior law required any person that conducts business in the state or that owns or licenses computerized data that includes personal information, or any agency that owns or licenses computerized data that includes personal information, to notify any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

New law deletes the requirement of prior law pertaining to persons conducting business in the state. Otherwise retains prior law.

Prior law required notification to be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, or any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the data system.

New law retains prior law and further requires that notification be made within 60 days of the discovery of the breach. Further provides that when notification is delayed the person or agency shall provide the attorney general with the reasons for the delay in writing within the 60 days period to receive an extension of time.

Prior law provided that notification may be provided by substitute notification if the person or agency demonstrates that the cost of notification would exceed $250,000 or that the affected class of persons exceeds 500,000, or the agency or person does not have sufficient contact information.

New law provides that notification may be provided by substitute notification if the person or agency demonstrates that the cost of notification would exceed $150,000 or that the affected class of persons exceeds 100,000, or the agency or person does not have sufficient contact information.

New law provides that notification shall not be required if after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to the residents of this state. Further, the person or business shall retain a copy of the written determination and supporting documentation for five years from the date of discovery of the breach of the security system.

New law provides that, if requested in writing, the person or business shall send a copy of the written determination and supporting documentation to the attorney general no later than thirty days from the date of receipt of the request.

Prior law (R.S. 51:1405(A)) declared unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce unlawful.

New law retains prior law and provides that violations of the Database Security Breach Notification Law constitute an unfair practice under R.S. 51:1405(A).

Effective August 1, 2018.

(Amends R.S. 51:3073(2) and (4)(a) and 3074)