

[Ariz. Rev. Stat. Ann. § 18-545](#)

Quick Facts

Breach Based on Harm Threshold	Deadline for Consumer Notice	Government Notification Required
YES	Most expedient manner possible without unreasonable delay	NO

More Details

Scope of this Summary	Notification requirements applicable to persons or entities that conduct business in the state and own, license, or maintain covered info. Some types of businesses may be exempt from some or all of these requirements and non-commercial entities may be subject to different requirements.
Covered Info	First name or first initial and last name, plus: Social Security number; driver's license or state identification card number; or financial account, credit or debit card number, in combination with any required security or access code or password that would permit access to a resident's financial account.
Form of Covered Info	Electronic Only
Encryption Safe Harbor	Statute does not apply to information that is encrypted, redacted, or secured by any other means rendering the element unreadable or unusable.
Breach Defined	Unauthorized acquisition and access that materially compromises the security or confidentiality of covered info maintained as part of a database of personal information regarding multiple individuals, and that causes or is reasonably likely to cause substantial economic loss to a resident, excluding certain good-faith acquisitions by employees or agents.
Consumer Notice	<u>Timing</u> : Must be made in the most expedient manner possible and without unreasonable delay consistent with any measures to determine the scope of the breach, identify residents affected, or restore the reasonable integrity of the system. <u>Method</u> : By written notice, telephone notice, or electronic notice if it is the primary method of communication with resident or is consistent with E-SIGN. Substitute notice is available if certain criteria are satisfied.
Delayed Notice	Notification may be delayed if law enforcement advises that notice will impede a criminal investigation.
Harm Threshold	Notification not required if, after a reasonable investigation, covered entity or a law enforcement agency determines a breach of the security of the system did not or is not reasonably likely to occur.
Third-Party Notice	If you maintain unencrypted computerized data that includes covered info on behalf of another entity, you must notify them without unreasonable delay following discovery of a breach. Must cooperate by sharing relevant information about breach.
Potential Penalties	Violations may result in civil penalties.

Last revised on May 30, 2018

This summary is for informational purposes only. It provides general information and not legal advice or opinions regarding specific facts. Additional requirements or conditions may apply to any or all provisions referenced herein. For more information about the state data breach notification laws or other data security matters, please seek the advice of counsel.