

Protection of Personal Information Act

Utah Code §§ 13-44-101, et seq.

- Any entity which conducts business in the State of Utah must prevent the unlawful use or disclosure of personal information they collect.
- Anyone who discovers a breach of their security system which relates to data containing personal information of a Utah resident must conduct an investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes.
- Under the Act personal information includes an individual's:
 - Social Security Number;
 - Driver's License Number;
 - State Identification Card Number;
 - Financial Account Number and Security/Access Code or Password; or
 - Credit or Debit Card Number and Security/Access Code or Password.
- If the investigation reveals that personal information was misused for identity theft or fraud, or misuse is reasonably likely to occur, notification must be made without unreasonable delay to each affected Utah resident. Notification may be made:
 - in writing by first-class mail to the resident's most recent address;
 - electronically, if the resident primary communicates electronically;
 - by telephone; or
 - if this notification is not feasible, by publishing the notice.
- In addition, if the misuse involves 500 or more Utah residents, notification must be made in the most expedient time possible to:
 - the Utah the Attorney General's Office; and
 - the Utah Cyber Center.
- If the misuse involves 1,000 or more Utah residents, notification must also be made to each nationwide consumer reporting agency that compiles and maintains files on consumers.