Security Breaches

How common are security breaches?

In 2011, at least 535 data breaches occurred in the United States. A conservative estimate of the number records affected by those breaches is 30.4 million.* In the wake of these breaches, business owners and managers across the country are reexamining their Information Security procedures.

Security Breaches affect businesses of all sizes—from the one-owner specialty shop to the largest international banking institutions. Accordingly, both Kansas and Federal laws provide guidance for businesses facing the possibility of a Security Breach. This pamphlet examines the laws regarding Security Breaches and provides tips for avoiding such breaches.

*Source: *Data Breaches: A Year in Review*. Privacy Rights Clearinghouse. https://www.privacyrights.org/top-data-breach-list-2011, last visited April 26, 2012.

What are some examples of security breaches?

- Computer hackers infiltrating a business' computerized records containing Personal Information from an undisclosed location.
- A business disposing of records containing Personal Information into a trash dumpster without properly destroying the Personal Information by shredding, erasing, or otherwise modifying the Personal Information in the records to make it unreadable or indecipherable through any means.
- A person stealing an unsecured company laptop containing Personal Information.

What laws in Kansas apply to security breaches?

In 2006 the State of Kansas erected safeguards designed to limit the damage caused by Security Breaches. K.S.A. 50-7a01 through 50-7a04 contain the relevant definitions and obligations related to Security Breaches in the State of Kansas. The Attorney General is empowered to bring an action in law or equity to address violations of these laws. Kansas law requires any person who conducts business in this state that owns or licenses computerized data including personal information to conduct good faith investigations into the likelihood that personal information has been or will be misused. K.S.A. 50-7a02.

If the investigation reveals that Personal Information has been misused, or is likely to be misused, the person must give notice to the affected Kansas resident as soon as possible. When a Security Breach requires notification of more than 1,000 consumers at a time, Kansas law requires the person to also notify all nationwide consumer reporting agencies of the Security Breach. K.S.A. 50-7a02. Keep in mind that law enforcement may determine it best to delay notice to a consumer if it is determined that the notice could impede a criminal investigation.

Kansas law requires a person or business to take reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the person or business. Specifically, Kansas law requires that such records be shredded, erased, or otherwise modified to make the personal information in the records unreadable or indecipherable through any means. K.S.A. 50-7a03.

What federal laws apply to security breaches?

Congress and Federal agencies have also passed laws and regulations concerning Security Breaches. A few examples of such laws are the Privacy Act, the Federal Information Security Management Act, Office of Management and Budget Guidance, the Veterans Affairs Information Security Act, the Health Insurance Portability and Accountability Act, the Health Information Technology for Economic and Clinical Health Act, the Gramm-Leach-Bliley Act, the Federal Trade Commission Act, and the Fair Credit Reporting Act.

These Federal Acts generally divide businesses into sectors (e.g. Health Care, Financial, Educational, etc.) and focus the requirements upon each sector's use of the protected information. The Federal Acts usually require covered entities to develop an information security policy and notify persons affected by breaches of such policy.

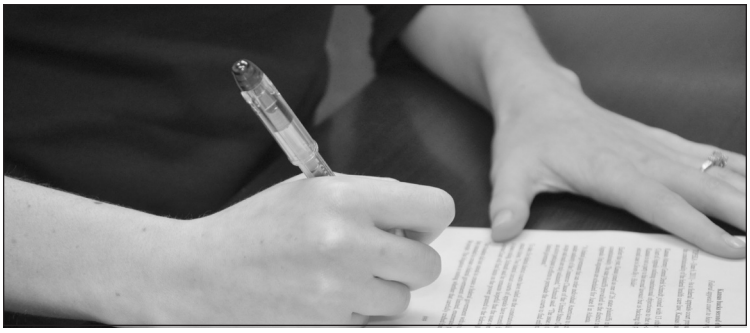
Tips to avoid security breaches

✓ Develop and implement a strong Information Security Policy

Good provisions for computer hard drives include password protection, encryption, firewall/antivirus software, and other common IT measures designed to limit exposure to a Security Breach. Physical records containing Personal Information should be locked in boxes and kept in secure locations.

✓ Ensure that employees follow the policy

A policy is only effective if it is followed. Each employee should understand and follow the business's Information Security Policy. The most proactive businesses incorporate job-specific training into the business' overall employee training regimen.



✓ Scale down

The less personal information around, the less vulnerable a business is to a Security Breach. Consider whether it is necessary for the business to keep credit card numbers and other personal information about customers.

✓ Keep an eye on the laptops

One common Security Breach occurs when an employee leaves their laptop in an unsecured area. To avoid this problem, control access to the business' laptops and ensure each employee keeps a vigilant watch over the business' computers. Password protection and encryption can also help with this type of breach.

✓ Properly dispose of Personal Information

Determine the length of time required for the business to maintain their records. If the business decides to dispose of Personal Information, be sure to take reasonable steps to destroy the Personal Information by shredding, erasing, or otherwise modifying the Personal Information in the records to make it unreadable or indecipherable through any means.

What to do if your data is breached

- Investigate the breach to determine whether Personal Information has been misused or is reasonably likely to be misused.
- Notify each affected Kansas resident in the most expedient time possible.
- Cooperate with law enforcement to determine whether notice should be delayed in order to avoid interfering with any criminal investigation.
- If circumstances require notifying more than 1,000 consumers at one time, notify the nationwide consumer reporting agencies of the timing, distribution, and content of the notices.

Provided by:

Kansas Attorney General

Derek Schmidt

120 SW 10th Ave, 2nd Floor
Topeka, KS 66612
Phone: (785) 296-2215 | Fax: (785) 296-6296
www.ag.ks.gov

For More Information

This pamphlet provides general information regarding Kansas and Federal law in this area. It is not to be relied upon as legal advice or guidance. It is important for businesses to determine their obligations and to comply with Kansas and Federal law. For more information regarding Security Breaches, please contact a private attorney.

June 2012