

# WASHINGTON'S SECURITY BREACH LAW

## NOTIFYING RESIDENTS



Every day, state and local government agencies collect valuable personal and financial information about Washingtonians. Residents expect that agencies will take reasonable precautions to keep their personal information safe, and agencies have a statutory duty to notify Washingtonians when a security breach puts that information at risk.

Following a string of high-profile data breaches, the Washington State Legislature recently passed [legislation requested by the Attorney General](#) to strengthen the state's data breach notification law ([RCW 42.56.590](#)). The intent is to help make sure that those affected receive necessary and timely information when a security breach occurs, and to copy the Attorney General's Office on such notification when there is a large-scale security breach. The new law is effective July 24, 2015.

### **What is a security breach?**

A security breach is the unauthorized acquisition of data that compromises the security, confidentiality, or integrity of personal information maintained by an agency.

For example, a security breach can occur by:

- A hacker electronically accessing and acquiring computerized data;
- Unauthorized access of a computer network through weak passwords;
- Unencrypted information sent through a payment system; or
- A briefcase or laptop computer containing client files that is stolen or misplaced.

### **What type of information does the law cover?**

The law covers breaches of personal information, which means someone's first name or first initial and last name in combination with *any* of the following:

- Social Security number;
- Driver's license number or Washington identification card number; or
- Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's account.

Personal information does not include information that is publicly available through a lawful request for public records.

### **When must affected individuals be notified of a security breach?**

Any state or local agency must notify Washington residents when a breach of personal information occurs that is reasonably likely to subject them to a risk of harm.

Washington residents *must* be notified if the information acquired and accessed was not secured during a breach or if the confidential process, encryption key, or other means to decipher the secured information was acquired by an unauthorized person.

Information is secured if it is encrypted in a manner that meets or exceeds the National Institute of Standards and Technology ([www.nist.org](http://www.nist.org)) standard or is otherwise rendered unreadable, unusable, or undecipherable by the unauthorized person.

**Office of the  
Attorney General  
BOB FERGUSON**

1125 Washington St. SE  
PO Box 40100  
Olympia, WA 98504  
360-753-6200  
[www.atg.wa.gov](http://www.atg.wa.gov)

**Consumer  
Resource Center**  
1-800-551-4636  
Monday-Friday  
10 a.m. to 3 p.m.

## **When must agencies deliver the notice of a security breach?**

Agencies are required to provide notification to residents about a security breach in the most expedient time possible and without unreasonable delay, and must provide notice no more than 45 days after discovering the breach.

Under limited circumstances, notification may be delayed upon request from law enforcement, or if additional time is needed to determine the scope of the breach or to restore reasonable integrity of the system.

## **How should the notice be provided?**

The notice must normally be provided in writing, which can be delivered electronically so long as it is consistent with federal law.

However, substitute notice may be provided if:

- The cost of notifying affected individuals would exceed \$250,000;
- More than 500,000 Washingtonians are affected; or
- The agency lacks sufficient contact information to provide written notice.

Substitute notice consists of email notification if possible, conspicuous posting of the notice on the agency's website, and notification to major statewide media.

## **What information must the notice include?**

The notice must be written in plain language and contain all of the following:

- The name and contact information of the agency reporting the breach;
- A list of the types of personal information that were, or are reasonably believed to have been, the subject of the breach; and
- The toll-free telephone numbers and addresses of the major credit reporting agencies.

## **When must the Attorney General's Office be notified?**

If a breach affects more than 500 Washington residents, an agency must notify the Washington State Attorney General's Office by electronically submitting a single sample copy of the security breach notification without any personally identifiable information. The sample should be sent before or at the same time notice is provided to affected individuals. The agency must also provide the number of Washingtonians affected by the breach, or an estimate if the exact number is not known.

Notifications to the Attorney General's Office can be submitted electronically at [SecurityBreach@atg.wa.gov](mailto:SecurityBreach@atg.wa.gov).

## **What happens if an agency fails to notify residents as required?**

Agencies that fail to provide notice as required under the law may be enjoined or liable to individuals for damages.

## **Are there any exemptions from the law?**

The law applies to all state and local agencies in Washington as defined in [RCW 42.56.010](#). However, agencies that provide notice as required under the Health Insurance Portability and Accountability Act have fulfilled their notification requirements to affected individuals under state law, but must still provide notice to the Attorney General's Office.