

## California Strengthening its Data Breach Notification Law

September 15, 2011 – California was the first state to require that companies notify consumers when their personally identifiable information is exposed without authorization; otherwise known as a “data breach”. And the state is widely known to have some of the strongest protections for consumer privacy in general. With the passage of Senate Bill 24, the state is strengthening those protections.

Tweet

```
(function() {  
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];  
s.type = 'text/javascript';  
s.src = 'http://widgets.digg.com/buttons.js';  
s1.parentNode.insertBefore(s, s1);  
})();
```

Any company doing business with California consumers – even if the company is located outside of California – is required to abide by the state’s data breach notification law. That law requires companies to notify consumers when “personally identifiable information” about them is leaked or stolen. And it defines “personally identifiable information” as a combination of data that includes the consumer’s full name or first initial and last name, along with any one of the following:

- Social Security number
- Driver’s License or State ID Card number
- Account numbers of any kind in combination with other data that would allow unauthorized individuals to access or use the affected account.
- Health insurance or medical information.

While notifications of data breaches have been a requirement in California for several years now, the content of those notifications was not mandated. The updated law changes this. Companies that experience a data breach will now be required to provide the following information:

- A contact name and phone number for the company reporting the breach.

- A list of all of the types of data that was breached. If the company is not sure, then it needs to provide a list of the types of data it reasonably believes were breached.
- The date of the breach.
- Any relevant information regarding delays in notification of the breach due to police investigations.
- A general description of the breach.
- And the names and toll free phone numbers for each of the major credit reporting agencies.

Companies will also be able to provide additional information as they deem necessary.

Any company that stores sensitive, personally identifiable information on consumers should have a written data breach notification policy. And because California's new requirements are currently the most rigid in the country, any company that does business in California should seriously consider adopting the California data breach notification standard when dealing with any data breach. For the moment, this will help to insure compliance with the myriad of state and local data breach notification laws.

by Jim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, [click here](#). Registration is easy and free.

Follow me on Twitter: