# Incident-Specific Web Site Template (Section Three)

**Other Toolkit Sections**

Toolkit Home | Section 1: Building a Press Release | Section 2: Notification Letter Components | Section 4: Incident Response FAQ | Section 5: Generic Identity Theft Web Site

## Template for Breach Notification Web Site

The information below will assist you in developing a breach notification web site. It is good practice to have a pre-built framework (skeleton site) in place that may need only appropriate and pertinent text information inserted into the page(s). This allows the expedient posting of breach information. Breach notification laws vary by state. The State Security Breach Notification Legislation/Laws is a good resource. Be sure you know what is required before there is a need to notify constituents of a breach.

## Common Elements

### Most-Recent-Update section at top of page

- Should include date/time stamps for each posting.

### Basic facts (*information that appears on the website should be exactly what's included in the notification letters and press releases*):

- **Who was impacted:** Students, employees, community
- **What data may have been involved:** Names/Addresses/email addresses, SSN's, unique student/employee ID's, etc.
- **When compromise or discovery occurred:** Date/Time: If the discovery indicates the breach happened some time ago, indicate that in the notification. It's important to be truthful.
- **Where compromise occurred:** A college, or specific unit, central IT, etc. Also include geographical location, if appropriate.
- **Whether anyone believed to be negatively affected or not:** A negative affect could be something as seemingly simple as requiring all employees to change their email password.

### Actions taken by unit/University to ensure more secure future/Ongoing measures

- Speak in layman's terms. Avoid technical terminology, if at all possible.

### How do I learn if I'm affected?

- If there needs to be further clarification as to exactly who was affected and who was not, put it here using different language. As example, "You are not affected, if . . .", as opposed to "You are affected, if. . ."
- If there is a way an individual can self-discover whether or not they are impacted, it is a good idea to include that information. Even constituents who were identified as NOT being affected will check anyway. It can be a "reassurance measure".

### Link to Identity Theft Web site/credit agencies

### FAQs

- FAQs should be part of the breach notification site. Keep them simple and reiterate what is on the main page. Reuse links if necessary.

### Press Releases

### Toll-free hotline contact information

## Where Site is Hosted/Located

- On Public Safety site
- On compromised unit's site
- On a specially dedicated "datatheft" Web site: www.univname.edu/datatheft
    - This places all data-related incidents in one place in chronological order; provides community members an easy-to-regularly-check place to look to see if they're affected.

## How Long Should Site Be Available

- It depends. There may be legal requirements involved that dictate length of time. Check with university counsel and your state's breach notification requirements.

---

Questions or comments? Contact us.