



Notifying Authorities and Constituents

The appropriate level of outside notification during a data breach depends on many factors, not the least of which is the university's legal position. The same policies that define critical incidents and systems should provide guidance on which data breach service providers and community contacts should be a part of the post-incident process.

Artifact E-F: Review your procedures and contact preparation with Experian's Preparedness Plan Audit (p. 22) and Sample Breach Vendor Contact Cards (p. 23).

While IT professionals understand the persistent challenges of data breaches, others involved may not react appropriately to incidents. Be prepared for a range of attitudes, from fear and anger to ambivalence.

Seek support from legal counsel and compliance units to pre-draft press release and victim notification language. This can expedite administrative tasks during a breach and ensure rapid response.

Artifacts H-I: This press release from the **University of Indiana** (p. 25) and sample notification letter from the **University of California at Irvine** (p. 26-28) provide representative templates.

Prepare to Move Past the Rolodex

Data Breach Services

- Forensic Investigators
- Private Investigators
- Outside Legal Counsel
- Mailing Services
- Call Centers
- Public Relations Firms

Community Contacts

- Law Enforcement
- Local Media Outlets
- Vendors Connected with Compromised Data
- Professional Organizations Affected by Breach

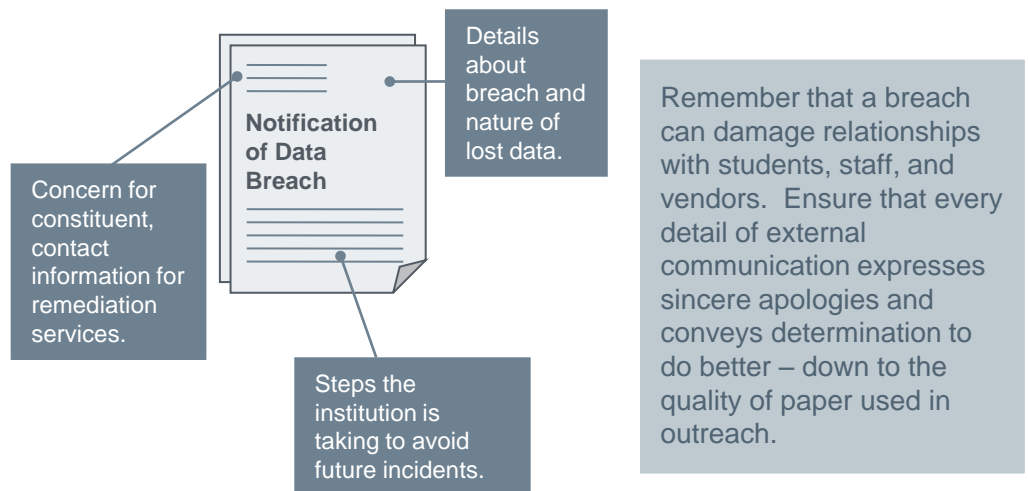


Keep All Response Leaders Updated with Key Contacts

Review lists of breach service providers and community contacts at least quarterly, and make sure all response leaders have accurate information when launching into team recruitment and investigation.

Strike the Right Tone

Sample Notification Letter



Artifact G: See more tips for Breach Communication on page 24.