SMITH, GAMBRELL & RUSSELL, LLP
Attorneys at Law

# A Data Breach Response Overview

| Process Step | Observations |
|---|---|
| **1. Secure or fix data loss or breach condition to the extent possible.** | This may require outside technical assistance. |
| **2. Notify insurance carrier.** | Even if there is no specific data breach insurance, a general liability policy may cover some costs. |
| **3. Engage counsel to assist with data breach compliance.** | There are often many compliance hurdles that must be met. Having counsel engage outside forensic analysts may entitle related reports to be covered by attorney work product privilege. |
| **4. Gather additional information about incident and audit scope of records involved, paying particular attention to personally identifiable or other sensitive information.** | This also may require outside assistance. Need to confirm the states of residence of any affected individuals. |
| **5. Consider filing a police report.** | Usually recommended and in some states this will be required to be made available to affected individuals. |
| **6. Based on data involved and states involved, assess data breach notification obligations – by statute (e.g., HIPAA, GLB, FTC privacy guidances, state laws) and by contract.** | Typically, done by outside counsel. If company is in a regulated industry (e.g., healthcare or banking) federal law often will prevail, but some state laws may be implicated. For non-regulated companies, the "patchwork" requirements of applicable state laws must be complied with. |
| **7. Provide notifications to affected individuals as required above.** | This can be costly and often outside mailing resources are needed. Need to assess offering of credit monitoring. |
| **8. Provide regulatory notices as required.** | Required in numerous states and at federal level in some cases. |
| **9. Assess system security and vulnerabilities and implement necessary remediation steps.** | Should be done on a parallel path to above and may be an issue in any later investigations and reports. |
| **10. Document incident and response steps taken for later audit.** | Often overlooked and not completed in the press of other matters, but documenting the incident and response is a best practice that will help later to defend decisions. |
| **11. Cooperate with any regulatory investigations or customer audits and address related issues on an ongoing basis.** | Customer relations and contractual obligations are often overlooked. |