Data Breach: From Discovery to Recovery

Aaron P. Simpson
Partner, Privacy and Cybersecurity Practice
Hunton & Williams LLP
(212) 309-1126; asimpson@hunton.com
Discovery

Alerts

Examples:
- Employee Report
- Customer Complaint
- Monitoring Tool Alert
- Subsidiary Notification
- Service Provider Notification
- Bank or Processor Report
- Law Enforcement Notification
- Media Request
- Intelligence Report

Internal Escalation

Example:
- Subsidiary reports to Parent
- InfoSec alerts Legal Dept.
- Incident Response Team Mobilized

Engagement

Examples:
- Forensic Examiners
- Outside Counsel
- Call Center Support
- Credit monitoring prov.
Investigation

Third-party forensic teams arrive onsite and commence forensic investigation

Travel Onsite

Acquisition & Preservation

Investigators preserve and forensically image relevant logs, databases and servers

Containment & Remediation

IT repairs, collects, disconnects, isolates, moves and/or rebuilds affected systems

Examination

- Deploy threat detection software
- Manually inspect logs and other evidence
- Search for indicators of compromise in forensic images
- Investigate attack vector

Ongoing Assessment of Nature and Scope of the Incident
Identify Affected Individuals

Scrub inaccurate or misformatted data
Correlate isolated data elements
Augment incomplete data
Remove duplicate data

List of Affected Individuals and Impacted Data

1. John Smith 123234414143323 0232
2. bobama@gmail.com 123456!
3. Homer Simpson 211-11-1221
4. Elvis Presley 656-43-4344

Data team then converts list of impacted individuals into a notification file
Legal Analysis

Determine potential legal obligations. Consider:

- State breach notification laws
- Federal Interagency Guidance
- HITECH Act

Generally triggered if:

Reasonable suspicion that PII has been accessed or acquired in an unauthorized manner
## Preparation of Notifications

Prior to the notification mailing or posting, the following steps typically must be taken:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>In-house or external call center is engaged and trained</td>
</tr>
<tr>
<td>2.</td>
<td>An IVR script is recorded if needed to handle the initial flood of calls to call center</td>
</tr>
<tr>
<td>3.</td>
<td>If credit monitoring or other identity protection services are being offered, retain a third party provider and provide it with notification file so it can produce and assign “redemption codes” to impacted individuals</td>
</tr>
<tr>
<td>4.</td>
<td>Identify regulator and CRA notification requirements based on the pool of affected individuals</td>
</tr>
</tbody>
</table>
Direct Notification

1. Legally-compliant notification letter and Call Center FAQs are prepared
2. If relevant, communication materials are translated into appropriate languages
3. The mailhouse vendor is engaged, as appropriate
4. Address information is run through a National Change of Address service to obtain latest contact information
5. Vendor (or internal mailhouse) prepares letter proofs and company reviews and approves them
6. Vendor (or internal mailhouse) customizes letters and populates them with relevant names and address information
7. Vendor (or internal mailhouse) prints and mails letters
Substitute Notification

Website notice, FAQs and Press Release are prepared.

If relevant, communication materials are translated into appropriate languages.

Website notice and FAQs are posted to company website homepage.

Press release is distributed to relevant media outlets.
Recovery

• Lessons Learned
• Respond to regulator follow-up inquiries
• Respond to lawsuits and contractual issues
• Evaluations
• Information Security Assessments
• Improvements
• Training and Testing