Checklist for Drafting a Breach Notification Policy

The following checklist can help you develop a Breach Notification Policy.

Individual(s) Responsible for Responding to a Security Breach

- Information Technology Systems employee
- Human Resources employee
- Legal Counsel
- Public Communications/Media Relations employee
- A security breach response team that includes representatives from more than one department

Action upon Learning or Being Notified of a Security Breach

- Immediately investigate the incident
- Isolate all affected systems to limit further data loss
- Contact the individual or team responsible for responding to the breach
- Determine whether law enforcement should be notified

Information to Collect Related to the Breach

- Date, time, duration, and location of breach
- How the breach was discovered, who discovered the breach, and any known details surrounding the breach, for example:
    - Method of intrusion
    - Entry or exit points
    - Paths taken
    - Compromised systems
    - Whether data was deleted, modified and/or viewed
    - Whether any physical assets are missing
- Details about the compromised data:
    - A list of affected individuals and type
    - Data fields
    - Number of records affected
    - Whether any data was encrypted (if so, which fields)
    - What personal information has been compromised
- Determine whether special consultants are necessary to capture relevant information and perform forensics analysis

Implications of the Breach

- Consider whether other systems are under a threat of immediate or future danger
- Determine whether you are legally obligated to provide notification about the breach and to whom
    - Residents of your state
    - Residents of other states
    - State agencies
    - Law enforcement
    - Credit reporting agencies
- Determine whether you are contractually obligated to provide notification about the breach
- Consult legal counsel regarding liability, litigation risk, law enforcement investigations, and other legal concerns

Procedures Follow in the Event that Written Notification Is Required or Elected

- Prepare a list of persons to be notified
- Choose a mode of communication for notification, if not already mandated by law
- Draft a notice that complies with applicable laws and contractual obligations
- Consider whether to offer certain remediation services to assist affected persons
- Be sure to comply with any legal or contractual timing requirements

Action Following a Breach and Notification

- Prepare an online FAQ and document inquiries and responses
- Review information technology systems and physical security
- Assess operational controls and consider revising company policies or procedures regarding data collection, retention, or storage
- Assess the need for additional employee training in data protection policies and processes
- Review agreements and policies to determine whether any updates or modifications need to be made, including agreements with third parties that handle personal information, website privacy notices and terms of service, agreements with customers or other third parties, and employee handbooks and policies
- Evaluate your response to the breach

* This checklist is provided by the National Association of REALTORS® in its *Data Security and Privacy Toolkit*. It is based on information found in the Federal Trade Commission's *Protecting Personal Information: A Guide for Business.*