Breach Notifications: How to Handle Breaches Across Jurisdictions

Moderated by: Zach Warren,
Editor-in-Chief, Legaltech News

States with/without breach notification laws

- 47 states, plus the District of Columbia, Guam, Puerto Rico and Virgin Islands, have breach notification laws
  (13 of these states have laws addressing security procedures)
- Alabama, New Mexico, and South Dakota do not have breach notification laws
- Recent developments

Regulator notification; paper format

- State breach notification laws require notification of a breach to affected individuals (25 of these laws, plus Puerto Rico law, require notification of a breach to state attorney general or regulator in addition to affected individuals)
- These laws cover breaches involving personal information in electronic format (10 of these laws cover breaches involving personal information in both electronic and paper formats)

Content requirements; timing

- 21 state breach notification laws have content requirements
  (4 of these laws cover identity theft prevention and mitigation services)
- 12 laws, plus Puerto Rico law, have specific notification requirements in terms of days

Personal information definition

- 12 state breach notification laws, plus Puerto Rico law, define personal information to include medical information (10 of these laws also define personal information to include health insurance information)
- 7 laws, plus Puerto Rico law, define personal information to include online account information

Other breach notification requirements

- Federal HIPAA / HITECH Act breach notification for covered entities and business associates regarding protected health information
- Will there be a comprehensive federal breach notification law?
- Laws in other countries
- Provisions in contracts and policies

Checklist of questions

- What happened? How and when did incident occur and how was incident discovered?
- Is law enforcement involved? Should law enforcement be contacted?
- Has there been any investigation (who)?
- Has the incident been contained, controlled or corrected (when and how)?
- Could any contracts or policies be implicated (are they available)?

Checklist of questions (con't)

- What security measures were in place before incident? What has been or will be done to decrease the risk of recurrence?
- What types of information are involved and in which format was the information?
- Is the information owned or licensed or maintained?
- Are there any indications of access to or acquisition of the information?

Checklist of questions (con't)

- What are residences of affected individuals (country? province?)? How many affected individuals reside in a given state? What are the state-specific notification requirements?
- What has been done to protect affected individuals? What steps can affected individuals take to protect themselves?
- Has a provider of identity theft prevention and mitigation services been engaged?
- Has any external disclosure been made (who, when and what)?

Mitigating Risk – Breach Response Plans

Taking steps to retain customers' trust reduces a breach's long-term financial impact. From the 2016 Ponemon Institute Study:

- *The longer it takes to contain a breach the more costly it becomes.* Breaches contained within 30 days of discovery cost an average of $5.24 million. If it takes more than 30 days to contain the breach, the average cost increases to $8.85 million.
- The average breach in 2016 cost $221 per record. Having an incident response plan and team in place, employee training, board-level involvement, and a Chief Information Security Officer in position are associated with reducing the cost of data breach to $56 per record.

Mitigating Risk – Breach Response Plans

Breach Response Plan Components

- Identify Team Leader(s) in charge of incident response
- Assign and establish team roles and responsibilities – legal, technical, public relations, etc.
- Specify incident handling procedures, strategy for deciding on the course of action, and procedures for communicating with organizational leadership and outside parties/law enforcement
- Conduct regular reviews

Resources

Cyber-Security Event Recovery Plan, Ransomware, State Breach Notification Law and Incident Response Plan Articles: https://www.irmi.com/biographies/melissa-krasnow

Written Information Security Programs:
http://www.vlplawgroup.com/blog/vlp-partner-melissa-krasnow-co-authors-two-resources-thomson-reuters-practical-law-written-information-security-programs-compliance-massachusetts-data-security-regulation/

IRS on Tax Scams / Consumer Alerts:
https://www.irs.gov/uac/tax-scams-consumer-alerts

Presenter information

Melissa Krasnow

Email: mkrasnow@vlplawgroup.com

Attorney biography:

http://www.vlplawgroup.com/attorneys/melissa-krasnow/

Presenter information

Robert E. Braun

JMBM Jeffer Mangels Butler & Mitchell LLP
jmbm.com

Email: RBraun@jmbm.com

Attorney biography:
http://www.jmbm.com/robert-e-braun.html