Welcome
Data Breach Summit

Ben Wright, Chair

Agenda and Housekeeping

Information Security Law and Politics Are Dangerous

- Data holder could include university, foundation, corporation, other non-profit or government entity
- Plaintiff lawyers want to make money
- Politicians and regulators want to attract attention and make examples
- The media want to attract viewers

Legal Standards Can Be Subjective & Open to Interpretation

- HIPAA Omnibus Rule 2013
- Incident presumed to be a breach UNLESS a risk assessment shows low risk of harm, recognizing
  - Was risk mitigated?
  - Was data actually viewed or downloaded?
  - Nature of the data and likelihood of identification

Legal Adversaries Can Disagree with Data Holder's Interpretation of Facts

- Reasonable minds can look at same facts and reach different conclusions.
- But adversaries may not be entitled to know about data holder's investigation and interpretation of the facts.

When You Have an Incident …

- You don’t know whether you had a “breach” requiring notice until you complete an investigation.
- Investigation can take time and sweat.
- Investigation might conclude no “breach” because (for example) no significant risk of harm.
- Or investigation might reach other conclusions that adversaries disagree with.

Data Holder Has Incentive to Keep Investigation Confidential

- First, limit who has knowledge of the investigation.
- Second, cloak investigation in “attorney work product” and/or “attorney-client privilege”
- “Attorney work product” prevents details of investigation from being disclosed under subpoena or lawsuit.

Genesco, Inc. v. Visa U.S.A., Inc.

- Retailer hires cyber investigators, under leadership of counsel, to investigate breach
- Later, in litigation, Visa demands investigators' reports
- Court denies Visa because reports constitute confidential "attorney-client communications" and/or "attorney work product"
- Confidentiality favors retailer