NAAG CONSUMER CHIEF
SPRING 2018: EVOLUTION OF
STATE DATA SECURITY AND
BREACH LAW

Monday, May 21, 2018

Jim Halpert, Co-Chair Global Privacy & Security Practice
DLA Piper US LLP
jim.halpert@DLAPiper.com
202-799-4441
State Data Security and Data Breach Law Overview

- Once Upon a Time in California (2002)
  - Environmental warning label analogy
  - Presented as warning consumers about risk of ID theft, fraud
  - Covers: name + SSN, government ID #, account number + access code
  - Then . . . 2005 Choicepoint breach → 39 states by 2010
  - 8 in this cohort have no harm trigger

- Second Generation Breach Notice Laws: some additional data elements, harm trigger
  - California adds medical, health insurance info (2008), account credentials, notice content requirements (2011)
  - NE, IA, WI add biometric data
  - More states add AG notice, some add content requirements (NC, MA)
  - All have harm trigger except contradictory language in MA
State Data Security and Data Breach Law Overview

- Third Generation Laws
  - In 50 states and DC, PR, USVI, Guam
  - Covering more data elements: adding medical, health insurance, biometric, online account credentials
  - Notice deadline: 45 or 60 days from determination breach occurred
  - AG notice at same time as state residents (need to file explanation in FL)
  - Acquisition of data standard (except FL) with risk of harm standard
  - Similar content requirements for notice to state residents (except for CA heading requirements)
  - Exceptions for entities with GLB or HIPAA breach notice obligations
Advice to Companies: Focus on the Big Picture

- Companies that do selective notification or hide significant breaches are more likely to get sued and to face significant fines.
- Actions with regard to citizens of 1 state often create precedent for citizens of other states.
- Absent an indemnification obligation, breach notice is chiefly a reputational issue.
  - The public understands by now that breaches happen by now → notify
  - Avoid jumping the gun with inaccurate notice
  - If it’s noteworthy, get notice out at one time if possible
  - Mention high level remedial steps already in progress to prevent future breaches
  - Some risk now to offering ID theft insurance – Remijas (CA7), Zappos (CA9)
State Outliers

- Data brokers alone must notify in GA
- Notice requirements for data elements of name + :
  - date of birth (ND), “shared secrets” (WY)
  - mother’s maiden name even if publicly available Hispanic surname, digital signature undefined (NC, ND),
  - information or combination of information that a person reasonably knows or should know would permit access to the consumer’s financial account (OR), “can be used” (NC)
- Notice content: right to obtain a police report (MA – often not relevant), rights under the FCRA (NM – often not relevant)
- Contradictory “risk of harm” language for a “data breach” but not for an unauthorized “disclosure” of personal data (MA – disclosures are less risky)
- “Should have known” of a breach or disclosure scienter standard (MA)
- Notifying multiple agencies in a single state (NJ -2, NY - 3)
State Data Security Requirements

- Reasonable security practices and procedures (majority rule)
- Gramm-Leach-Bliley Act Safeguards Rule Approach (procedural -- OR)
- Nudges toward encryption
  - Exception to breach notice (majority of states are tech neutral, though)
  - NV: safe harbor from civil liability if encrypted PI when it is outside premises
  - MA: information security program, including encryption of PI outside premises and on laptops and other portable devices, plus other measures
  - NYDFS: more extensive information security program including governance and encryption or compensating controls
Aligning Protecting Data with Cybersecurity

- Cybersecurity is extremely difficult, dynamic threats, nation state actors, CIA/DoD/NSA have all been hacked, enterprise-wide challenge
  - Significant implications for operations and even for job (trade secret theft)
- Protecting personal data is one part of a strong cybersecurity program
- Breach notice is already very effective at imposing significant costs -- $200 per notifiable record (Ponemon Institute)
  - But if non-sensitive information must be notified, this distorts security incentives
  - Classic example: Payment card data already subject to PCI-DSS, minimal risk to consumers but it is radioactive and gets disproportionate emphasis
- State data security requirements create similar incentives, should be tailored
- Plaintiffs’ bar (CA), card issuing bank proposals would create greater distortion
Federal Data Security/Breach Notice Requirements

- Financial services entities regulated by federal functional regulators - NPI
- HIPAA covered entities AND business associates - PHI
- Telecomm carriers - CPNI
- Federal Government contractors – government data and contractors’ systems
- Other critical infrastructure
- NIST Cybersecurity Standard
  - Flexible to threats facing the enterprise
  - Data is one asset that may be targeted but far from the whole picture
  - Scale-able and can flow down to contractors
  - Compatible with int’l standards (eg ISO) and becoming an int’l standard