Once More Unto the Breach: Litigating the Aftermath of Cyberknaves’ Invasions

INSURANCE AND FINANCIAL SERVICES LITIGATION – WEBINAR SERIES

Robert D. Owen
Mark Thibodeaux
Tracey K. Ledbetter

November 17, 2015
Speakers

Robert D. Owen
212.389.5090
robert.owen@sutherland.com

Mark Thibodeaux
713.470.6104
mark.thibodeaux@sutherland.com

Tracey K. Ledbetter
404.853.8123
tracey.ledbetter@sutherland.com
Once more unto the breach, dear friends, once more;
Or close the wall up with our English dead.
In peace there’s nothing so becomes a man
   As modest stillness and humility:
But when the blast of war blows in our ears,
   Then imitate the action of the tiger;
Stiffen the sinews, summon up the blood,
   Disguise fair nature with hard-favour’d rage . . .

(William Shakespeare, Henry V)
Recent examples of settlements

- Heartland Payment (130mm) - $1 million settlement
  - $60 million settlement with Visa
- Target Consumer MDL (110mm) - $10 million settlement
  - $6.7 million in fees to the lawyers
- Target / Visa (40mm) - $67 million settlement
  - Earlier $19 million settlement rejected by MasterCard issuers
- Sony Gaming Networks (24mm) - $1 million cash, $14 million non-cash
- Schnuck Markets (2.4mm) - $2.1 million settlement
- LinkedIn (50k) - $1.25 million settlement
Litigation Issues

• Public announcement of a data breach WILL bring class actions and other litigation.

• Possible claims by…
  ▪ Consumers and individuals whose private data is stolen
  ▪ Credit card issuers: For violation of the PCI Data Security Standard
  ▪ Vendors and third parties: Who is at fault?
  ▪ Shareholders
    ▪ Securities litigation
    ▪ Director and officer litigation / derivative suits
  ▪ You: For insurance coverage
Litigation Issues

- Hurdles for consumer plaintiffs may include...
  - Lack of injury
  - Standing
  - Causation
  - Damages
Litigation Issues: Standing?

• Until recently, consumer plaintiffs faced significant hurdles in proving actual injury on motion to dismiss.

• *Remijas v. Neiman Marcus Group*, 794 F.3d 688 (7th Cir. 2015): Reversed dismissal of putative class action for lack of standing.
  - “The injuries associated with resolving fraudulent charges and protecting oneself against future identity theft” are sufficient to satisfy the requirement of injury in fact.
  - Petition for hearing *en banc* denied.

• The Supreme Court may provide guidance on the injury in fact requirement during the upcoming term.
  - *Spokeo, Inc. v. Robins*, No. 13-1339
After the Breach…

• Retain a forensic expert
• Prepare for litigation: e-discovery
• Check insurance coverage
• Notification and disclosure
• Enforcement and litigation

… or Before the Breach
Litigation and eDiscovery

• eDiscovery implications
  ▪ Litigation hold – to issue or not to issue
  ▪ What to save – network logs?
  ▪ What to save – internal communications regarding the breach
  ▪ What to save – evidence pertaining to negligence
Litigation and eDiscovery

- Reducing litigation risk
  - Document retention: Are you retaining too much?
  - Employee education and training (e.g., phishing)
  - Vendor oversight
  - Testing / auditing of security
  - Evidence preservation: What don’t you have to retain and what should you retain?
Insurance Coverage: Which Policies Might Apply?

- Cyber insurance policies
- Business property (first-party) coverages
  - Covers direct *physical* loss
- Commercial general liability (CGL) policies
- Personal and advertising injury coverages
- Employee dishonesty / fidelity policies
Insurance Coverage: Purchasing Cyber Risk Coverage

- Defending claims resulting from:
  - Network and data security breaches
  - Regulatory investigations
  - Judgments and settlements

- Limits of liability / policy period
  - Retroactive coverage date
  - Cost of coverage may be increasing
Insurance Coverage: Purchasing Cyber Risk Coverage

- Consider covering costs of:
  - Notifying individuals whose data has been breached
  - Providing credit monitoring
  - Retaining public relations and forensic investigation consultants
  - Restoring lost or stolen data
  - Pursuing indemnity rights when someone else has caused the breach
  - Lost revenue due to interruption of business operations
  - “E-ransom” demands
Notification and Disclosure

• **Laws**
  - Gramm-Leach-Bliley Act
  - Several enacted in December 2014
    - The National Cybersecurity Protection Act of 2014
    - The Cybersecurity Enhancement Act of 2014
  - No information-sharing liability protection (yet)

• **Proposed bills and executive action**
  - Uniform data breach notification requirement
    - 47 different state laws on privacy and data protection
  - Legislation to encourage information-sharing

• **Law enforcement?**
Enforcement

• Bad cybersecurity as an unfair or deceptive trade practice
  ▪ Not providing the security you promise = deceptive
  ▪ Not providing adequate security = unfair

• Consent orders can get expensive
  ▪ 20 years of security assessments
  ▪ LabMD – the cost of fighting enforcement

• Violation of consent orders
  ▪ Google was fined $22.5 million
Enforcement: *Wyndham*

  - 15 U.S.C. § 45(a) prohibits “unfair or deceptive acts or practices in or affecting commerce.”
  - Does this statute give the FTC authority to regulate cybersecurity?
    - Yes!
      - No actual injury requirement
      - Statute provides sufficient notice
      - *Start with Security: A Guide for Business*

- What about state unfair trade practices acts?
Litigation: Claims Asserted to Date

- Fair Credit Reporting Act
- Common law right to privacy
- Breach of contract (or implied contract)
- Unjust enrichment
- Breach of fiduciary duty
- Negligence, gross negligence, negligent misrepresentation
- State statutory violations, including consumer fraud / unfair trade practices statutes
Litigation: Other Potential Claims

- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act
- *Parens patriae* claims by State Attorneys General
- State notification statutes
  - 47 states and the District of Columbia have enacted laws requiring notice of security breaches of personal data.
Litigation: Defenses

- Lack of standing
- Failure to state a claim
- Failure to show causation
- No private right of action
- Not negligent / best practices followed
- Contribution (poorly chosen customer passwords)
Questions?

Robert D. Owen
212.389.5090
robert.owen@sutherland.com

Mark Thibodeaux
713.470.6104
mark.thibodeaux@sutherland.com

Tracey K. Ledbetter
404.853.8123
tracey.ledbetter@sutherland.com