Strafford

Presenting a live 90-minute webinar with interactive Q&A

Data Privacy Class Actions: Navigating Latest Legal Theories, Leveraging Defense Strategies, Evaluating Insurance Coverage

THURSDAY, FEBRUARY 2, 2017

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Natasha G. Kohne, Partner, **Akin Gump Strauss Hauer & Feld**, Abu Dhabi, United Arab Emirates

Linda D. Kornfeld, Partner, **Kasowitz Benson Torres & Friedman**, Los Angeles

Donna L. Wilson, Partner, **Manatt Phelps & Phillips**, Los Angeles

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-866-869-6667** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 35.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

manatt

Data Privacy Class Actions: Navigating Latest Legal Theories, Leveraging Defense Strategies, Evaluating Insurance Coverage

Presented by:

Donna L. Wilson

dlwilson@manatt.com

February 2, 2017

OUTLINE

- Limiting Litigation Risk Before A Risk Arises
- Data Breach Response: Think Like a Litigator
- The State of Information Security and Privacy Litigation Today
  - Pre-*Clapper*
  - *Clapper*: The Final Word?
  - Now Comes *Spokeo*…
  - Post-*Spokeo*: Be Careful What You Wish For
  - Security Breach Litigation
  - Class Certification Issues in Privacy and Data Breach Litigation
  - Privacy/Data Breach Litigation Settlements
  - Privacy and Data Security Class Action Settlements
  - Avoiding Class Action Suits – Arbitration Provisions
- Takeaways

LIMITING LITIGATION RISKS BEFORE A RISK ARISES

- In-house and outside counsel coordination with other stakeholders in identifying and mitigating litigation risk.
  - Product and Service Development
  - Contracts with Business Partners, Vendors, and Vendor Oversight
  - Indemnification and Insurance
  - Information Security Audits and Risk Self-Identification
  - Information Security and Response Planning

DATA BREACH RESPONSE: THINK LIKE A LITIGATOR

- Planning Ahead
- Forensics and the Privilege
  - *In re: Target Corp. Customer Data Security Breach Litig., 2014 WL 1338473 (MDL 2014)*
  - *Genesco, Inc. v. Visa U.S.A., Inc., 2015 WL 5297903 (M.D.Tenn. 2015)*
- Notice
- Monitoring and Standing

THE STATE OF INFORMATION SECURITY AND PRIVACY LITIGATION TODAY

- Is *Clapper* the final word, or a pyrrhic victory, on the issues of standing?
- Does standing even matter if you're faced with (or wielding) a statutory damages claim?
- If data is the new oil, will data breach and privacy become the new asbestos? Litigation and settlement trends.

- Putative Data Security/Privacy Class Actions – risk of harm, cost to mitigate, loss of value
  - *Lambert v. Hartman*, 517 F.3d 433 (6th Cir. 2008) (finding standing where plaintiff's information was posted on a municipal website and then taken by an identity thief, causing actual financial loss fairly traceable to the defendant's conduct).
  - *Resnick v. AvMed, Inc*., 693 F.3d 1317 (11th Cir. 2012) (standing where plaintiffs had both been identity theft victims).
  - *Pisciotta v. Old National Bancorp*., 499 F.3d 629 (7th Cir. 2007) (finding standing in a security breach class action suit against a bank based on the threat of future harm).
  - *Krottner v. Starbucks Corp*., 628 F.3d 1139 (9th Cir. 2010) (finding standing in a suit where plaintiffs unencrypted information (unencrypted names, addresses and social security numbers of 97,000 employees) was stored on a stolen laptop, based on possibility of future harm).

Pre-*Clapper* (cont'd)

- Putative Data Security Class Actions – risk of harm, cost to mitigate, loss of value (cont'd)
  - *Reilly v. Ceridian Corp*., 664 F.3d 38 (3d Cir. 2011) (finding no standing in a suit by law firm employees against a payroll processing firm alleging negligence and breach of contract relating to the risk of identity theft and costs to monitor credit activity), cert. denied, 132 S. Ct. 2395 (2012) - distinguished environmental and toxic tort cases.
  - *In re LinkedIn User Privacy Litig*., 932 F. Supp. 2d 1089 (N.D. Cal. 2013)

Clapper: The Final Word?

- Differences among circuits regarding sufficiency of injury for purposes of standing (present v. future injuries).
- Game Changer? - *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (Feb. 26, 2013)
  - Threatened injury must be "certainly impending" to constitute injury-in-fact.
  - The Court, however, re-affirmed *Monsanto Co.* v. *Geertson Seed Farms*, 130 S. Ct. 2743, 2754-55 (2010) ("reasonable probability" or "substantial risk" sufficient for standing).
- Effect of *Clapper* on data breach litigation
  - Plaintiffs have taken the position *Clapper* is limited to the facts. Defendants have relied upon *Clapper* to challenge standing based upon possibility of damages, steps taken to prevent future damages (i.e., future risk of identity theft, incurring costs for credit monitoring services). With a few exceptions, Defendants are winning…

Clapper: The Final Word? (cont'd)

- *In re Barnes & Noble Pin Pad Litigation, No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013)* – relying on Clapper, dismissing class action for lack of standing. Rejected various theories of injury, including Barnes & Noble's failure to promptly notify plaintiffs of security breach; increased risk of identity theft; and time and expenses incurred to mitigate risks of identity theft.
- *Galaria v. Nationwide Mut. Ins. Co., 998 F. Supp. 2d 646 (S.D. Ohio 2014)*
- *Remijas v. Neiman Marcus Group*, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014)
- *Lewert v. P.F. Chang's China Bistro Inc.*, 819 F.3d 963 (7th Cir. 2016)
- *Cheatham v. ADT Corp.*, 161 F. Supp. 3d 815 (D. Ariz. 2016)
- *Moyer v. Michael's Stores, Inc.*, No. 14 C 561 (N.D. Ill. July 14, 2014) (dismissing claims for breach of implied contract and state consumer fraud statutes based on Michael's alleged failure to secure their credit and debit card information during in-store transactions).
- *Polanco v. Omnicell, Inc*., 2013 WL 6823265 (D.N.J. Dec. 26, 2013)- relying on *Clapper*, dismissing class action for lack of standing. Plaintiffs did not allege either misuse of plaintiffs' PCI or PHI and court rejected theories of injury including increased risk of identity theft and time and effort to mitigate.

Clapper: The Final Word? (cont'd)

- *But see, e.g.,*:
  - *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, MDL 11MD2258 AJB MDD, 2014 WL 223677 (S.D. Cal. Jan. 21, 2014) (pre-dating *Gallaria*)
  - *In re Adobe Systems, Inc. Privacy Litigation*, No. 13-CV-05226-LHK (N.D. Cal. Sept. 4, 2014) (relying on *Krottner*, and distinguishing *Clapper* and *Gallaria*)
  - *In re Google, Inc. Privacy Policy Litigation*, 2014 WL 3707508 (N.D. Cal. July 21, 2014)
  - *In re SAIC Corp.*, 45 F. Supp. 2d 13 (D.D.C. 2014)

Now Comes *Spokeo*…

- *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016) (Alito) (compromise 6-2)
  - The fact that plaintiff states a claim under a federal statute that does not require a showing of injury or damage does not mean that the plaintiff has standing.
  - "Particularization is necessary to establish injury in fact, but it is not sufficient. An injury in fact must also be 'concrete.'" Concrete means "'real,' and not 'abstract.'"
  - Intangible injuries may be concrete. In determining whether an intangible harm constitutes injury in fact, both history and Congress play important roles.
    - Does an alleged harm have "a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts"?
    - Congress may elevate to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law. However, "Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right. Article III standing requires a concrete injury even in the context of a statutory violation."
  - Significantly, the Court acknowledged that the risk of real harm could satisfy standing in appropriate circumstances

Post-*Spokeo*: Be Careful What You Wish For

- *E.g., Medellin v. Ikea U.S. West Inc.*, No. 15-cv-55174, 2017 WL 128112 (N.D. Cal. January 13, 2017)
  - In Song-Beverly case, vacating and directing trial court to dismiss without prejudice, where plaintiff strategically conceded that she did not suffer concrete harm under Federal law sufficient to confer Article III standing, and argued that her case therefore belonged in state court.

- Claims don't always fit well into existing federal statutes – CL and state statutes
- Is there any damage or loss?
- Can the plaintiffs establish causation?
- At the same time – certain expanding concepts of duty and breach
  - *Patco Construction Co. v. People's United Bank*, 684 F.3d 197 (1st Cir. 2012) (holding defendant's security procedures to not be commercially reasonable)
  - *Anderson v. Hannaford Brothers Co*., 659 F.3d 151 (1st Cir. 2011)
    - Allowing negligence, breach of contract and breach of implied contract claims to go forward
    - Implied contract by grocery store to undertake some obligation to protect customers' data
    - Class certification denied: *In re Hannaford Bros. Co. Customer Data Sec. Breach Litigation*, 293 F.R.D. 21 (D. Me. 2013)
  - *Lone Star National Bank v. Heartland Payment Systems, Inc*., 729 F.3d 421 (5th Cir. 2013)

- Proving Predominance Is Key
  - *E.g., In re Hannaford Bros. Co. Customer Data Sec. Breach Litigation*, No. 08-md-1954, 293 F.R.D. 21 (D. Me. Mar. 20, 2013)
    - Denied motion for class certification. Plaintiffs had failed to offer expert opinion testimony regarding class wide damages.
    - Instructive for plaintiffs in the future on how to overcome issue of individualized damages?
- E.g., Class Certification Rare But Possible in Privacy Litigation
  - *Harris v. comScore*, No. 11-cv-5807, 292 F.R.D. 579 (N.D. Ill. Apr. 2, 2013)
    - Certified a class based on claims comScore gathered and sold customers' personal information without their consent, alleging violations of the Stored Communications Act, Electronic Communications Privacy Act, Computer Fraud and Abuse Act
    - Class consisted of all individuals who have downloaded and installed comScore's tracking software onto their computers via one of comScore's third party bundling partners at any time since 2005
    - The Seventh Circuit denied comScore's petition for an interlocutory appeal on June 11, 2013
  - *Welch v. Theodorides-Bustle*, 773 F. Supp. 2d 692 (N.D. Fla. 2010) (DPPA case certified)

Privacy/Data Breach Litigation Settlements

- Sufficient relief for class members?
  - *Fraley v. Facebook, Inc*., No. 11-cv-1726, 2013 WL 4516819 (N.D. Cal. Aug. 26, 2013)
    - Approving $20MM settlement arising from alleged misappropriation of users' names and/or likenesses to promote products and services through Facebook's "Sponsored Stories" program. Original proposed settlement did not win preliminary approval
  - *Marek v. Lane*, 134 S. Ct. 8 (2013), Chief Justice Roberts, in an opinion denying certiorari, still took the time to explain his views on the limits and applicability of cy pres tools to settle cases
- Claims by customers who did not suffer identity theft
  - *Resnick v. AvMed Inc*., No. 10-cv-24513 (S.D. Fla. Feb. 28, 2014)
    - Granted final approval of $3MM data breach settlement. Claims can be made by both customers that paid defendant for insurance and customers who suffered identity theft caused by the breach

- Statutory damages: Where the Real Money Used to Be. *But see Spokeo.*
  - E.g., comScore: Illinois federal judge granted final approval of a $14 million settlement of putative class claims that comScore, a web measurement firm, violated various privacy statutes by collecting usernames and passwords, search queries, and credit card numbers, among other data, through allegedly bundling its tracker software with free downloadable games and products, and without providing notice or obtaining consent from consumers

Avoiding Class Action Suits – Arbitration Provisions

- Arbitration and Class Action Waivers

TAKEAWAYS

- Privacy and Data Security should be top areas of focus for enterprise risk management and information governance
  - Settlement values are arguably rising, and more plaintiffs' counsel are getting into the game
  - Regulatory attention also is increasing
  - Risks are rising
- "Bake" privacy and data security into your corporate culture and business
- Review your risks regularly, and devise strategies to avoid or minimize them

Akin Gump
STRAUSS HAUER & FELD LLP

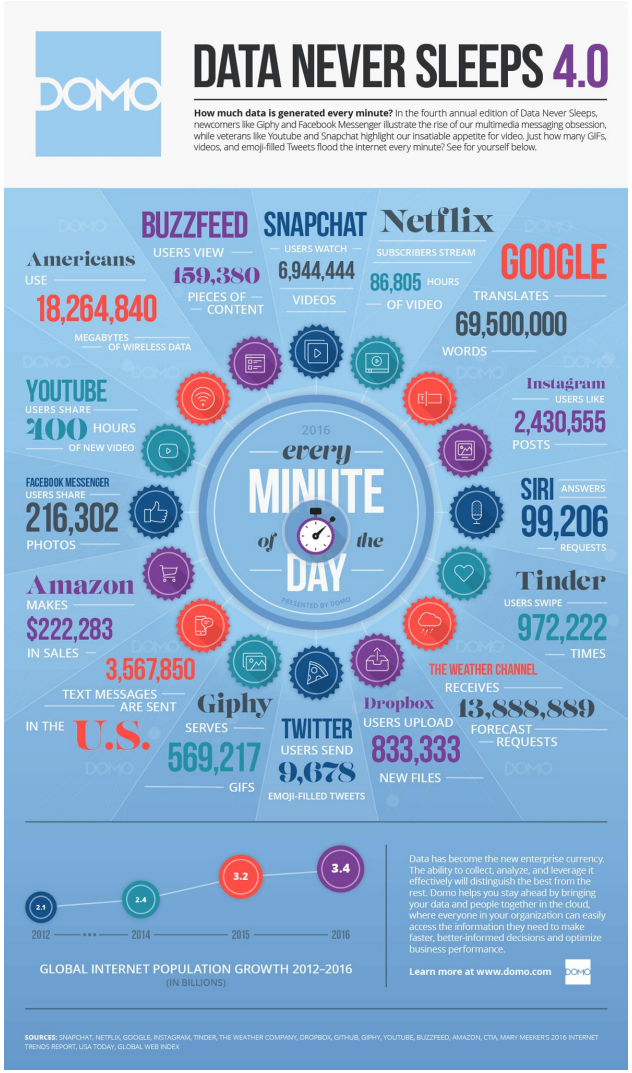
Data Privacy Class Actions: Navigating Latest Legal Theories, Leveraging Defense Strategies, Evaluating Insurance Coverage

Potential New Areas of Risk and Reward

Natasha Kohne, Partner, San Francisco
nkohne@akingump.com

Big Data: Big Problems for Business and Big Opportunities for Plaintiffs?

- What is big data?
  - According to the FTC – The term "big data" refers to a confluence of factors, including the nearly ubiquitous collection of consumer data from a variety of sources, the plummeting cost of data storage, and powerful new capabilities to analyze data to draw connections and make inferences and predictions.



Big Data: Legal Vulnerabilities That Plaintiffs May Exploit

Areas of opportunities for plaintiffs

- Employment
  - Sensitive health or genetic information (e.g., disability, race) can be used by employers in hiring practices
- Finance / loan
  - Effect on credit ratings, credit worthiness
  - Lack of affordable access to credit
- Healthcare / insurance
  - Potential for eligibility determinations or discrimination in premiums
- Educational
  - Potential for discrimination in admission decisions based on, e.g., race, family income

Big Data: Legal Issues

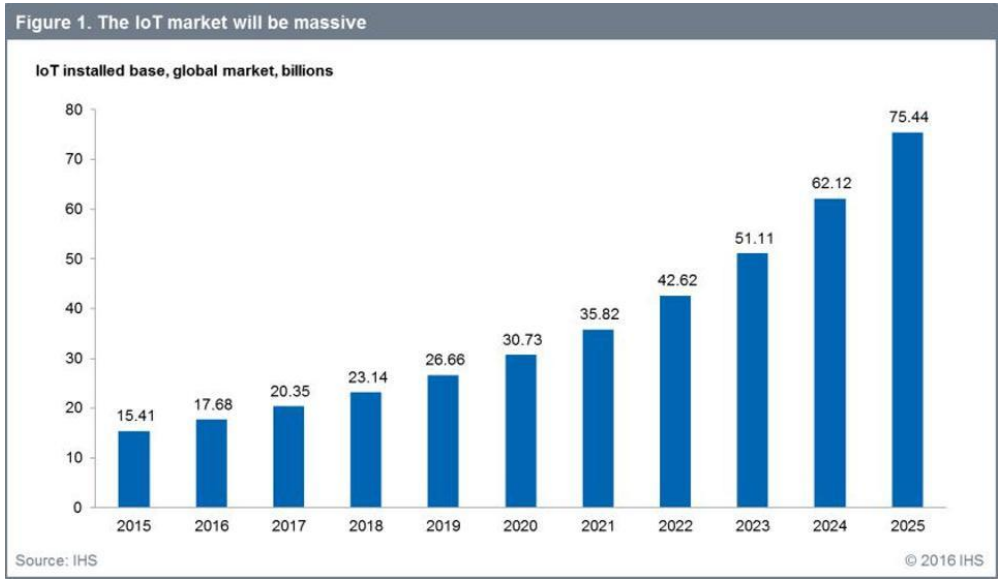
- FCRA
- Antidiscrimination laws
  - Title VII of the Civil Rights Act of 1964
  - Americans with Disabilities Act
  - Equal Credit Opportunity Act
- Federal Trade Commission Act

Big Data: Compliance Considerations

- How representative is your data set?
  - Missing information
- Does your data model account for biases?
  - Review data sets for biases
- How accurate are your predictions based on big data?
  - Correlation may not be meaningful
  - Profiting from misleading or inaccurate information (i.e., selling misinformation)
  - Problematic algorithms that are protected as trade secrets
  - Need for human oversight
- Does your reliance on big data raise ethical or fairness concerns?

The Internet of Things: Assessing the Risks

- 30B+ Internet of Things devices by 2020
  - IHS forecasts that the IoT market will grow from an installed base of 15.4 billion devices in 2015 to 30.7 billion devices in 2020 and 75.4 billion in 2025.
  - McKinsey estimates the total IoT market size in 2015 was up to $900M, growing to $3.7B in 2020 attaining a 32.6% compound annual growth rate (CAGR).
- Types of smart devices
  - Home appliances
  - Fitness trackers
  - Home security
  - Vehicle trackers
  - Medical devices
  - Cities



The Internet of Things: Regulatory Concerns

Federal Trade Commission

- September 2013: settled with TRENDnet, a marketer of **video cameras**, for "lax security practices" that allegedly "exposed the private lives of hundreds of consumers to public viewing on the Internet"
- November 2013: IoT Workshop
- January 2015: FTC Report on IoT, providing guidance and best practices for businesses in the IoT, based on the conversation at its workshop.
- February 2016: settled with ASUSTek Computer, Inc. for alleged "critical security flaws in its **routers** [that] put the home networks of hundreds of thousands of consumers at risk"
- January 2017: lawsuit filed against D-Link for alleged failure to take reasonable steps to secure its **routers and IP cameras**

"The Internet of Things holds great promise for innovative consumer products and services. But consumer privacy and security must remain a priority as companies develop more devices that connect to the Internet." – Former FTC Chairwoman Edith Ramirez (Sept. 2013)

The Internet of Things: Regulatory Concerns

- State Attorneys General
  - In October 2016, the California Attorney General advised Californians "to protect their electronic devices from potential hacks" and urged IoT manufacturers and developers "to take immediate steps to help secure home electronic devices against capture by a potential 'botnet attack.'"
- Congressional Actions
  - January 2015: Senate Committee on Commerce, Science and Transportation called for regulations of the IoT at a hearing. Senator Cory Booker (D-NJ) encouraged growth of the IoT over restriction.
  - November 2016:
    - Senator Richard Blumenthal (D-CT) urged the FTC to take action to ensure the security of the IoT and "to hold accountable any IoT manufacturers that fail to implement reasonable security standards."
    - Representatives Frank Pallone (D-NJ) and Jan Schakowsky (D-IL) on the U.S. House of Representatives' Committee on Energy and Commerce urged the FTC to "call on IoT device manufacturers to implement security measures" and "alert consumers to the security risks posed by continuing to use default passwords on IoT devices."

The Internet of Things: Best Practices

- Best practices – "reasonable security"
  - "security by design" by building security into devices at the outset
  - Privacy or security risk assessments, considering risks presented by collection and retention of consumer information
  - Data minimization
  - Security testing before product launch
  - Employee training
  - Vendor management and oversight
  - Consider "defense-in-depth" approach where security measures are considered at several levels, e.g., encryption
  - Reasonable access control measures
  - Continuous monitoring throughout product lifecycle
  - Notice and choice (consistent with context of transaction)

Potential Game Changers: FTC and AG Actions and Future Developments

Pre-Trump Administration / Obama Administration

- Privacy and data security comes to the forefront
  - FTC Start with Security guide
  - Over 60 data security enforcement actions
  - Comments to and impact on FCC proposed rulemaking
  - Solidified FTC authority to regulate data security
  - Increased enforcement by other regulators

Trump Administration

- New FTC Chairwoman Maureen Ohlhausen (R) appointed last week
- Two additional Republican seats and one Democratic seat to be filled
- Unclear whether enforcement actions will continue at same rate
- Potential challenges to FTC authority to regulate data security

Potential Game Changers: FTC and AG Actions and Future Developments

State Attorneys General and Other State Regulators

- Potential for stronger focus of regulatory action at the state level, given potential de-regulation at the federal level
- California
  - 2016 Data Breach Report: minimum level of reasonable security
  - New attorney general in office, can expect continued vigorous enforcement
- Connecticut
  - First state to affirmatively require businesses to provide security services to consumers:
    - requires all businesses, including health insurers, who experience data breaches to offer 1 year of identity theft prevention to affected individuals at no cost to them
- New York Department of Financial Services
  - First state to regulate cybersecurity practices
  - Proposed regulations become effective March 1, 2017

Potential Game Changers: FTC and AG Actions and Future Developments

- Potential new legislation
  - Federal level
    - Nationwide data breach notification statute
  - State level
    - Expanding definition of “personally identifiable information” to include geolocation
    - Increased regulation of biometrics
  - International Level
    - Privacy Shield
- Increased Litigation?
  - Privacy advocates find other avenues

Potential Game Changers: FTC and AG Actions and Future Developments

- Open questions
  - What is reasonable security?
  - What is the definition of personal information and what are our rights surrounding personal information?
  - What is considered harm or injury?
  - How will Europe react?

KASOWITZ

KASOWITZ BENSON TORRES & FRIEDMAN LLP

Data Privacy Class Actions: Navigating Latest Legal Theories, Leveraging Defense Strategies, Evaluating Insurance Coverage

Linda D. Kornfeld

Kirsten C. Jackson

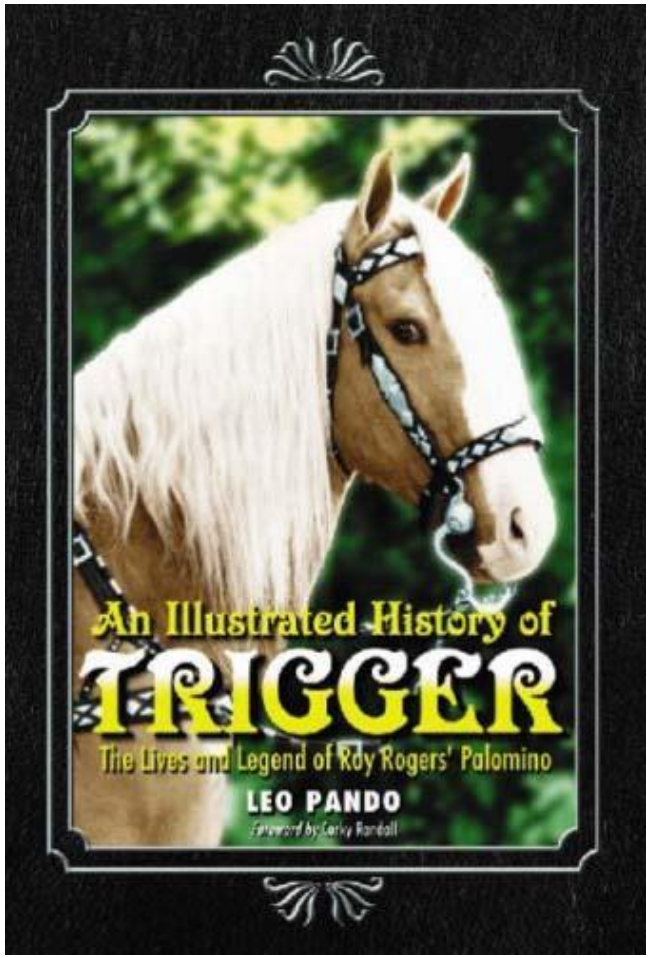
Data Breach, Privacy and Cyber Risks: Illustrative List of Costs

- **First Party Costs**
  - Forensic Examination/ PCI/ PFI Audits
  - Privacy Notification Costs
    - Privacy counsel
    - Mailing
    - Notification
  - Credit Monitoring/ Call Center Services
  - Business Interruption
  - Intellectual Property Loss
  - Public Relations
  - Extortion
- **Third Party Costs**
  - Claims by Private Litigants
    - Consumers
    - Other businesses
  - Claims by State Attorneys General
  - Claims by FTC
  - Regulatory Fines & Penalties
  - PCI Fines & Penalties
  - Loss of Business
  - Damage to Reputation

Overview: Insurance Coverages at Stake

- Crime – rogue employee
- Directors & Officers
- Errors & Omissions
- Property
- General Liability Coverage
- AND “Cyber” or “Privacy” Liability

First Step: Audit traditional coverages to see what may be triggered . . .



Possible Coverage Gaps

- Property Insurance – Tangible vs. Intangible
- D&O – Property exclusion; Professional services exclusion; investigations often not covered by insuring clauses
- Crime/Fidelity policies –Tangible Property
- CGL – ISO Exclusions for losses associated with unauthorized access by third parties
- E&O – Often exclude security breaches or damages arising from unauthorized access
- EPL policies – Often not covered by Insuring Clauses

General Liability – Overview

- Policyholders seek to obtain CGL coverage not only for privacy suits following a data breach, but also for their substantial exposures under agreements that may allow credit card processors such as Visa, Discover and MasterCard to impose charges on them in the event of a data breach.
- Courts have split on these issues.
- Focus is on Coverage B (Personal and Advertising Liability).

General Liability (cont.)- Coverage B

- "Coverage B" covers "those sums that the insured becomes legally obligated to pay as damages because of 'personal and advertising injury.'"

- "Personal and advertising injury" is defined to mean "injury … arising out of one or more of the following offenses:
  - … [o]ral or written publication, in any manner, of material that violates a person's right of privacy."

General Liability (cont.)- Coverage B

- The early cases addressing data breach, privacy and other cyber claims under CGL coverage are mixed.

- To the extent coverage is found, it has been limited to certain fact settings and to certain types of exposures. CGL coverage does not encompass all data breach, privacy and cyber losses -- even when courts find some coverage.

General Liability (cont.)- Coverage B

Hartford Cas. Ins. Co. v. Corcino & Assocs., No. CV 13-3728 GAF (JCx), 2013 WL 5687527 (C.D. Cal. Oct. 7, 2013).

- The insured allegedly posted "private, confidential, and sensitive medical and/or psychiatric information" on a public website, which remained online for almost a full year. Patients brought class actions which sought, among other relief, statutory damages of $1,000 per person under the California Confidentiality of Medical Information Act ("CMIA") and statutory damages of up to $10,000 per person under the California Lanterman Petris Short ("LPS") Act.
- The insurer contended coverage was barred under an exclusion for "Personal and Advertising Injury ... [a]rising out of the violation of a person's right to privacy created by any state or federal act." However, the court found that the plaintiffs in the underlying cases seek remedies for breaches of privacy rights that were not themselves 'created by any state or federal act,' but which exist under common law and the California state Constitution.
- The court also rejected Hartford's argument that statutory penalties are not covered "damages" because of "personal and advertising injury," finding that "[t]he statutes … permit an injured individual to recover damages for breach of an established privacy right, and as such, fall squarely within the Policy's coverage."

General Liability (cont.)- Coverage B

Travelers Indem. Co. v. Portal Healthcare Solutions, LLC, No. 1:13-cv-00917-GBL-IDD (E.D. Va. Aug. 7, 2014).

- Insured allegedly posted "confidential medical records" on a public website, and patients (who later sued) alleged that they were able to access those records by way of a simple Google search.
- The court ruled:
  - There was "publication" because the records were "place[d] before the public," rejecting the insurer's argument that the insured did not intend to publish the information.
  - The posting of the records without security restriction could give "unreasonable publicity" to and cause "disclosure" of information about patients' private lives, rejecting the insurer's argument that information could only be "disclosed" if it were viewed by third parties.
- Thus, the insurer had a duty to defend the insured in the underlying class action.
- The Fourth Circuit Court of Appeals affirmed the lower court ruling in 2016.

General Liability (cont.)- Coverage B

Zurich Am. Ins. Co. v. Sony Corp. of Am., No. 651982/2011 (N.Y. Sup. Ct. Feb. 21, 2014).

- Sony's PlayStation Network was hacked in April 2011. The hackers stole personally-identifiable information of over 77 million users, one of the largest data breaches in history.
- Sony argued that hackers' theft of personal information fell within the Coverage B offense of "oral or written publication in any manner of material that violates a person's right of privacy."
- The court ruled that coverage was not triggered where the "publication" offense was not an intentional act committed by the insured, but instead was the result of a criminal act of a third party hacker. The offense requires "an act by or some kind of act or conduct by the policyholder in order for coverage to be present," it held.
- This case settled while on appeal to New York intermediate appellate court.

General Liability (cont.) – Coverage B

Recall Total Mgmt., Inc. v. Fed. Ins. Co., 83 A.3d 664 (Conn. Ct. App. 2014)

- Insured transport vendor allegedly lost data tapes containing sensitive data on a large number of employees. Those tapes allegedly were recovered by a third party, but there was no evidence that the information on the tapes was ever accessed. The main "damages" sought were the costs of notification and remedial measures allegedly taken by the party who owned the data tapes.
- Court ruled that there was no "publication" absent evidence that information on the tapes was ever accessed, noting that the communication of information to a third party was required to trigger coverage.
- The court also held that triggering a breach notification statute does not demonstrate personal injury as such statutes "merely require notification to an affected person so that he may protect himself from potential harm."

CGL – ISO Endorsements

In 2014, ISO introduced endorsements addressing the access or disclosure of confidential or personal information:

- *CG 21 06 05 14 (Exclusion – Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability – With Bodily Injury Exception)*
  - Excludes coverage, under Coverages A and B, for injury or damage arising out of any access to or disclosure of any person's or organization's confidential or personal information
  - Exclusion will apply even if damages are claimed for notification costs, credit monitoring, forensics, etc.
  - Includes a limited bodily injury exception arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data
- *CG 21 07 05 14 (Exclusion – Access Or Disclosure Of Confidential Or Personal Information And Data-Related Liability – Limited Bodily Injury Exception Not Included)* - Very similar to CG 21 06, but does not include bodily injury exception

Possible CGL Coverage Still Available?

- Companies may face significant risk if they hope to rely upon CGL policies for coverage of data breach claims

- According to a recent Marsh & McLennan survey, last year 39% of private companies believe that their CGL policy provides at least some cyber coverage

Potential Coverage Under Crime Policy

May Cover:

- Loss of money, securities or property caused by criminal acts of third parties
- Loss of money or securities resulting from fraudulent fund transfer
- Loss resulting from employee dishonesty
- Credit card fraud
- Associated expenses

May Not Cover:

- Indirect or consequential loss (*e.g.*, phishing)
- Loss of confidential information
- Loss of intangible or intellectual property
- Fines and penalties

- *Retail Ventures, Inc. v. National Union Fire Ins. of Pittsburgh, Pa.,* 691 F.3d 821 (6th Cir. 2012). The court found coverage under the computer fraud rider of blanket crime policy for expenses for customer communications, public relations, lawsuits, regulatory defense costs, and fines imposed by credit card companies)

Potential Coverage Under Crime Policy

Apache Corp v. Great American Ins., 2015 WL 7709584 (S.D. Tex. 2015)

- Crime policy included computer fraud coverage if a loss directly resulted from the use of any computer ”to fraudulently cause a transfer of [money] from inside the premises”
- Secretary at insured received fraudulent email claiming to be from a vendor seeking a change to bank account to which Apache made payments to vendor
- Another Apache employee called the number on fraudulent letterhead to verify, the fraud perpetrator verified, and $2.4 million was sent to the fraudulent account
- Insurer argued that the loss did not directly result from the computer, asserting that the “use” of a computer was merely incidental to the fraudulent scheme (as all other steps did not involve a computer)
- The court disagreed, finding coverage because the fraud was a “substantial factor” in causing the loss (despite the involvement of employees), noting that the Fifth Circuit had previously found that the term “cause directly” is synonymous in meaning to the tort concept of “cause in fact”
- Case is on appeal to the Fifth Circuit Court of Appeals

Bank of Bellingham v. BancInsure (8th Cir. 2016)

- Financial institution bond contained computer systems fraud coverage
- Secretary at insured forgot to turn off computer overnight, which was then accessed by hackers
- The insurer denied coverage, taking the position that the secretary was the cause of the loss
- The court disagreed, finding coverage because the hacking was the proximate cause

Potential Coverage Under D&O

- Data breach may lead to an investigation or an enforcement action by the SEC or DOJ
- Gov't investigations may not trigger coverage because of how the investigations are conducted (*e.g.*, document subpoenas)
- D&O policies frequently contain a standard exclusion for privacy violations and data breaches
- Many D&O policies also contain exclusions for "terrorism", "war", "government action" – this could bar coverage for a cyber incident, depending how it arose

"Cyber" Policies

- Cyber and privacy exposures are ever evolving and claims scenarios are often complex.
  - *E.g.*, Hollywood Presbyterian Hospital computers locked for over a week based upon a ransomware attach—were insiders involved? How did the perpetrators get access? Is there coverage?

- As Cyber risks evolve, the need to purchase cyber coverage increases, and if the coverage previously has been purchased, careful underwriting is critical upon each annual renewal.

"Cyber" or "Privacy" Liability Policies:

- **May Cover:**
  - *First party costs*
    - Forensic Examination/PCI/ PFI Audits
    - Privacy Notification Costs
      - Privacy counsel
      - Mailing
      - Notification
    - Credit Monitoring/ Call Center Services
    - Public Relations
    - Extortion/Ransomware
  - *Third Party Costs*
    - Claims by Private Litigants
      - Consumers
      - Other businesses
    - Claims by State Attorneys General
    - Claims by FTC
    - Regulatory Fines & Penalties
    - PCI Fines & Penalties

May Not Cover:

Loss of Business

Damage to Reputation

There is a variation in products in the marketplace.
Each policy is subject to its own terms, conditions, limitations and exclusions.

Considerations for Purchasing Cyber Coverage

- Identification of your risk of exposure
- Involve stakeholders in the purchase renewal process: privacy and other in-house counsel, CIO, CTO – and even the C.
- Policies are complex with multiple definitions—carefully review to confirm that definitions match business risks.
- ISO exclusions, case law limitations, and evolving risk and associated expenses mean companies need to think about buying specialty coverage.

Potential Exclusions in Cyber Policies

- Unencrypted devices/servers
- Failure to update software / maintain security protections
- Acts of War/Terrorism
- Limitation to losses in the United States
- Breaches not related to electronic records
- Bodily injury / Property Damage
- Copyright/Trademark Infringement/Patent
- Breach of contract or warranty

Cyber Coverage Litigation

- There have been very few cases addressing coverage under “standalone” cyber insurance policies.

- Possible reasons for the lack of cyber coverage litigation:
  - Some companies remain resistant to purchasing standalone coverage
  - Cyber insurance industry is still relatively new, with a lack of uniformity of policy language
  - Apparent (though not quantified) lack of widespread denials of coverage

- As more companies purchase cyber coverage, the amount of cyber coverage litigation will undoubtedly increase.

Cyber Coverage Litigation: PCI Fines

P.F. Chang's v. Federal Insurance, 2016 U.S. Dist. LEXIS 70749 (D. Ar. May 31, 2016)

- Chang's suffered a June 2014 data breach involving 60,000 credit cards
- MasterCard assessed $1.9 million in PCI assessments to the payment processor, who sought to pass that to Chang's pursuant to their contract
- Federal provided $1.7 million in coverage for forensics and defense costs for claim made by customers and a bank, but denied the $1.9 million PCI assessments
- Chang's tried to argue that these PCI obligations would have arisen in the absence of the contract, as these assessments were the "functional equivalent" of compensating the victims of the breach.
- The court's overall conclusion was that two exclusions and the definition of loss were found to bar coverage for all assessment:
  - One exclusion was for liability assumed under contract,
  - The other exclusion (and definition of loss) excluded costs or expenses for "any obligation assume by, on behalf of, or with the consent" of Chang's.
- The court said it was unable to find any evidence that Chang's would have liable for these assessments absent the contract (so no exceptions to the exclusion applied)
- P.F. Chang's has filed an appeal to the Ninth Circuit.

Cyber Coverage Litigation: PCI Fines

New Hotel Monteleone LLC v. Certain Underwriters at Lloyd's of London (E.D. La. No. 2:16cv00061).

- Insured contends that it had deficient PCI liability coverage following a cyberattack in October 2014.
- Policy had $3 million in general limits, but coverage for PCI fines was sub-limited to $200,000
- Insured sued both insurers and the retail agent, alleging negligence failure to procure the correct coverage and breach of contract
- Thereafter, the retail agent filed a third-party complaint against a specialty broker (which worked on placement), which had professed expertise in the area of cyber insurance

Cyber Coverage Litigation: PCI Fines

Spec's Family Partners, Ltd. v. Hanover (S.D. Tex., No. 16cv438).

- The Insured, a retail chain, fell victim to an attack on its credit card payment network.
- Following two data breaches, MasterCard issued two liability assessments totaling nearly $10 million upon the company processing payments for the insured. That company made a demand on the insured for indemnification.
- The insured filed suit against the processing company in Tennessee federal district court for breach of contract.
- Hanover purportedly refused to pay for the cost of the litigation against the payment processing company.
- The insured then filed suit against Hanover, alleging breach of the policy and bad faith and seeking a declaratory judgment action.
- Hanover has filed a motion for judgment on the pleadings (under seal)

Potential Coverage Issues: "Minimum Security Requirements"

- Some cyber policies may require the insured to follow "minimum required practices" regarding network security, which in some instances is stated as a "condition precedent" to coverage.
- Exemplar language: "The Insured warrants, as a condition precedent to coverage, that it shall: (1) follow the Minimum Required Practices that are listed in the Minimum Required Practices endorsement as a condition of coverage under this policy; and (2) maintain all risk controls identified in the Insured's Application and any supplemental information provided by the Insured in conjunction with Insured's Application for this Policy."
- ***However***, often the "exclusion does not apply to "negligent" or "unintentional" circumvention of controls.
- *See Columbia Casualty Co. v. Cottage Health System*, No. 2:15-CV-03432 (C.D. Cal.).

Potential Coverage Issues: Third-Party Coverage

- Does the policy apply to data losses involving third-party vendors or data stored in the cloud?
- Do such vendors have adequate coverage?
- What about additional insured status under such policies?
- In addition to reviewing your own coverage, should you conduct a similar analysis and require modifications to your trading partners' coverage?

Potential Coverage Issues: Consultants and Counsel

- Does the policy allow the insured to hire its own: (1) consultants to address forensics and other issues in response to a breach event, and/or (2) defense counsel?
- Exemplar language:
  - "The Insurer will select and appoint defense counsel."
  - "As a result of notification of a breach, the Insured shall be contacted by a designated Breach Consultant who shall gather information from the Insured and assess the severity of the Privacy Wrongful Act. After this evaluation, the Breach Consultant shall provide the Insured with guidance on how to respond to the Privacy Wrongful Act. Breach consultants shall be attorneys from the firm of [an insurer-side law firm]. . . The Breach Consultant shall represent the Insured throughout the breach response process . . . Including determining the applicability of the Insured's obligation to comply with any Breach Notification law, and if necessary, managing all third party service providers, preparing notification letters . . . And messaging for . . . Regulatory entities, the media and other entities."

Potential Coverage Issues: The "Application"

- How broadly does the policy define "application"?
- The issue: if any information or documents provided to the insurer during the procurement process later is determined to be inaccurate, the insurer may be able to deny all coverage for data breach expenses or litigation.

Potential Coverage Issues: The "Application"

- Exemplar language:

"The Insureds represent that the statements contained in the Application, and any materials submitted or required to be submitted therewith are the Insured's representations, are true . . . This Policy shall be null and void if the Application contains any misrepresentation or omission: a. made with the intent to deceive, or b. which materially affects either the acceptance of the risk or the hazard assumed by the Insurer under the Policy."

"**Application**" means:

"all signed applications for this Policy and for any policy in an uninterrupted series of policies issued by the Insurer. Application includes any materials submitted or required to be submitted therewith."

"the signed application, information, statements, representations, attachments and exhibits submitted to the Insurer in connection with the underwriting of the Policy or any other policy of which this Policy is a renewal."

Potential Coverage Issues: Investigation of a Potential Breach

- Does the policy pay for expenses incurred to investigate a potential breach of your network?

- Many policies cover a “cyber security” or “data” and associated expenses, but the definitions of these events do not include a “reasonably suspected” unauthorized access to or acquisition of data from your network.

CONCLUSIONS

- Although most cyber coverage disputes have dealt with "traditional" insurance policies, the industry has taken affirmative steps to eliminate exposure for cyber claims under CGL and other traditional policies.

- While litigation over coverage under traditional policies will still continue, courts are now seeing more coverage litigation involving cyber policies (which appears to be the trend going forward).

- Nevertheless, as *PF Chang's* shows, courts will likely still employ the same policy interpretation rules used in relation to traditional policies when interpreting cyber policies.

- Given the lack of uniformity of cyber policies, insureds (and their agents/brokers) are best served by confirming the scope/terms of coverage during the underwriting process to avoid future coverage disputes.

Questions?

Linda D. Kornfeld
lkornfeld@kasowitz.com
(424) 288-7902

Kirsten C. Jackson
kjackson@kasowitz.com
(424) 288-7905