

The logo for K&L GATES, featuring the company name in white, uppercase, sans-serif font on a dark blue rectangular background.

K&L GATES

A background image showing a dense array of fiber optic cables. The cables are illuminated from within, creating a vibrant green and teal glow. The perspective is from a low angle, looking up at the cables as they fan out across the frame, creating a sense of depth and technological complexity.

## What You Need To Know About Defending Cyber-Related Class Action Litigation

January 15, 2015

## PRESENTERS



**R. Bruce Allensworth**  
Partner, K&L Gates Boston  
+1.617.261.3119  
[bruce.allensworth@klgates.com](mailto:bruce.allensworth@klgates.com)



**Andrew C. Glass**  
Partner, K&L Gates Boston  
+1.617.261.3107  
[andrew.glass@klgates.com](mailto:andrew.glass@klgates.com)



**Roberta D. Anderson**  
Partner, K&L Gates Pittsburgh  
+1.412.355.6222  
[roberta.anderson@klgates.com](mailto:roberta.anderson@klgates.com)




**Matthew G. Ball**  
Partner, K&L Gates San Francisco  
+1.415.249.1014  
[matthew.ball@klgates.com](mailto:matthew.ball@klgates.com)



**Joseph C. Wylie**  
Partner, K&L Gates Chicago  
+1.312.807.4439  
[joseph.wylie@klgates.com](mailto:joseph.wylie@klgates.com)

# TOPICS

- Coordinating with Data Breach Response Team
- Theories of Injury Raised by Consumers and Credit Institutions in Response to Data Breaches
- Statutory and Common Law Causes of Action Typically Pleaded in Data Breach Related Class Actions
- Approaches to Defending Claims and Opposing Class Certification
  - Motions to Dismiss for Lack of Standing or for Failure to State a Claim
  - Opposing Motions for Class Certification
- Lessons Learned from Past Data Breach Class Actions
- Insurance Coverage Considerations
- Q & A



# Coordinating with the Data Breach Response Team

# COORDINATING WITH THE DATA BREACH RESPONSE TEAM

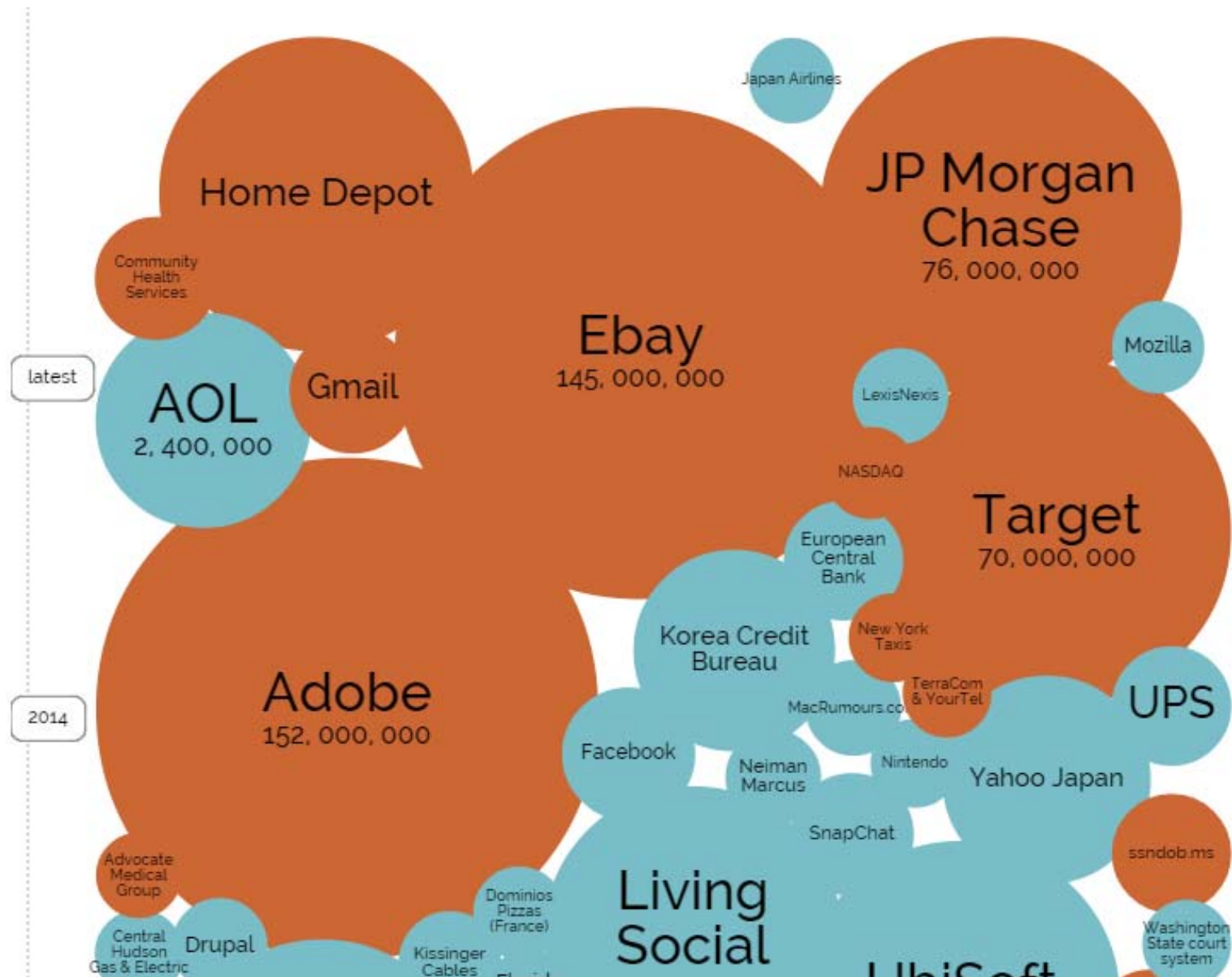
- How To Achieve Cyber-Reliance in the Face of Increased Risk and Exposure
  - The Last 18 Months
  - The Next 60 Days
  - **The First 24 Hours**
- Notice Requirements





# THE LAST 18 MONTHS

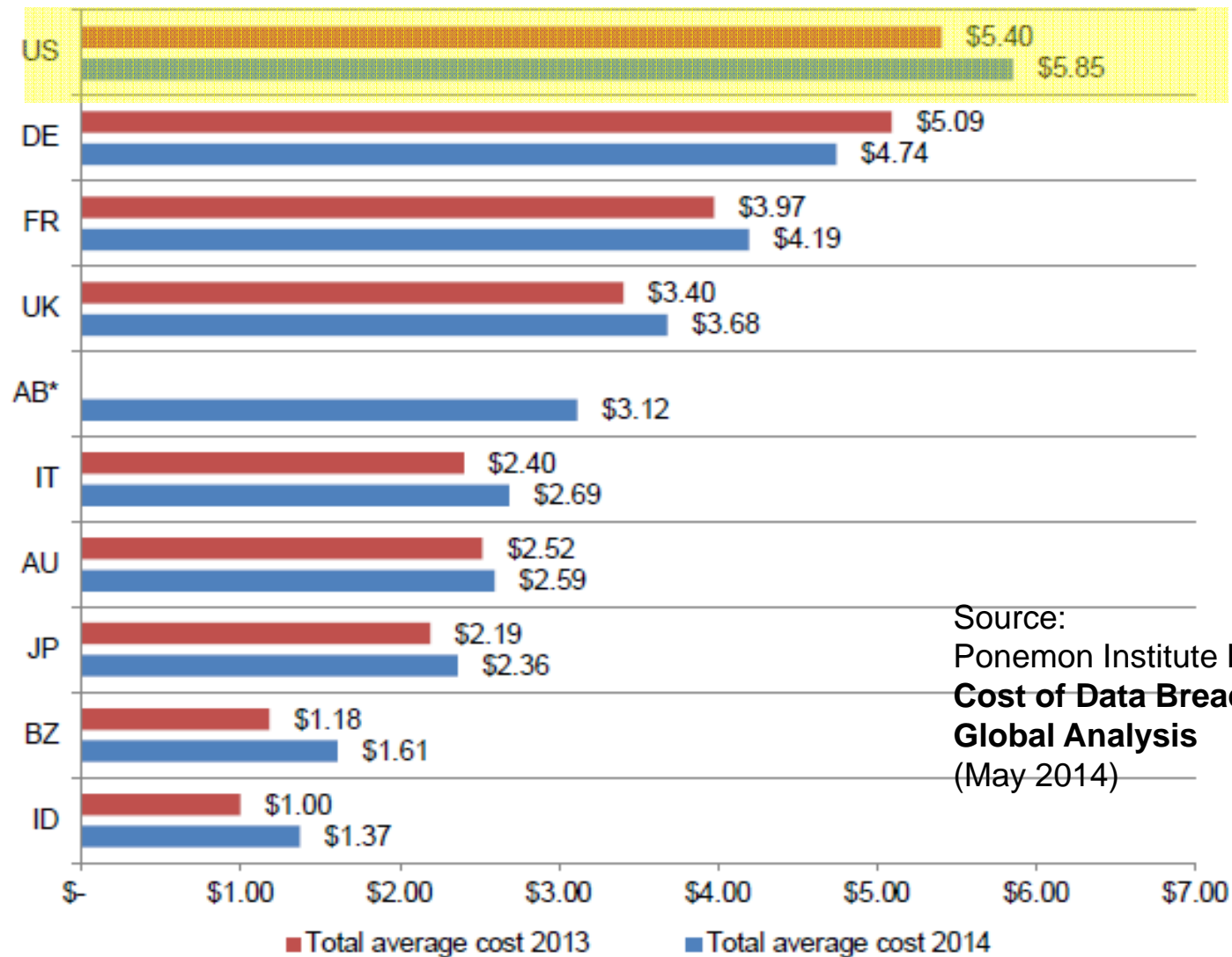




<http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>



**Figure 3. The average total organizational cost of data breach over two years**  
 Measured in US\$ (\$000,000 omitted)

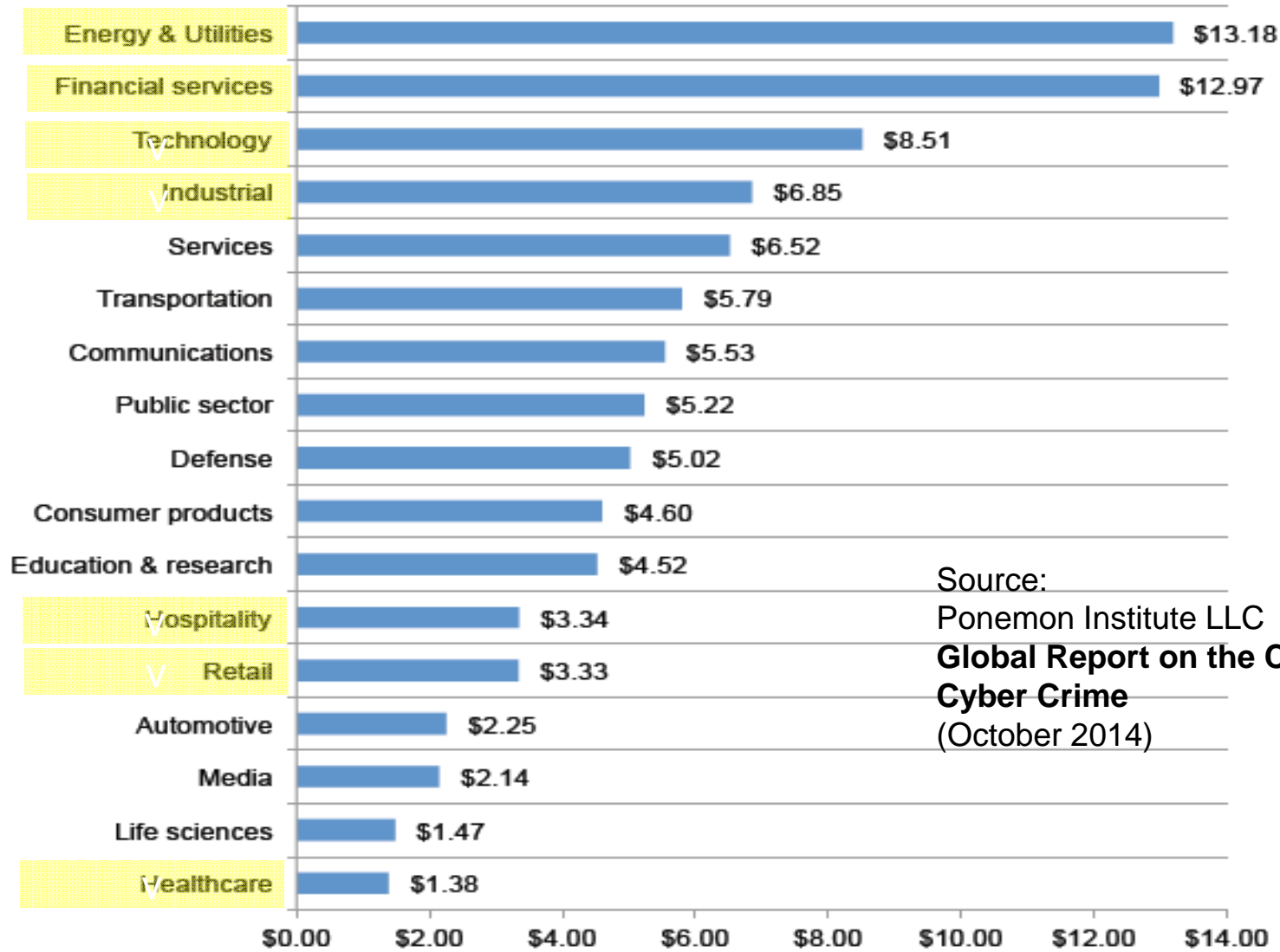


Source:  
 Ponemon Institute LLC  
**Cost of Data Breach Study:  
 Global Analysis**  
 (May 2014)

\* Data not available for FY 2013

**Figure 7. Average annualized cost by industry sector**

Cost expressed in US dollars, \$1,000,000 omitted  
 Consolidated view, n = 257 separate companies



Source:  
 Ponemon Institute LLC  
**Global Report on the Cost of  
 Cyber Crime**  
 (October 2014)



# THE NEXT 60 DAYS

## THE NEXT 60 DAYS

- How To Become Cyber-Resilient
  - C-Suite Attention
  - Cybersecurity Assessment
  - Compliance Review
  - Breach Response Plan
  - Employee Training
  - Vendors
  - Information Governance
  - Insurance

## THE NEXT 60 DAYS



- **Factors that decreased and increased the cost of a data breach.** Having a strong security posture, incident response plan and CISO appointment reduced the cost per record by \$14.14, \$12.77 and \$6.59, respectively. Factors that increased the cost were those that were caused by lost or stolen devices (+ \$16.10), third party involvement in the breach (+ \$14.80), quick notification (+ \$10.45) and engagement of consultants (+ \$2.10).

Source:  
Ponemon Institute LLC  
**Cost of Data Breach Study:  
Global Analysis**  
(May 2014)





# THE FIRST 24 HOURS

# THE FIRST 24 HOURS

- Don't panic. Follow the plan.
  - Mobilize First-Response Team
  - Immediately Call Breach Coach Counsel
  - Forensics
    - Investigate, Isolate, Contain, and Secure Systems / Data
    - Preserve Evidence
    - Document Everything
  - Public Relations
  - Consider Contacting Law Enforcement

# THE FIRST 24 HOURS

## Don't Panic.

1. Record the date and time of discovery and time when response efforts begin.
2. Alert and activate everyone on the response team, including external resources, to begin executing your preparedness plan.
3. Investigate, while preserving evidence.
4. Stem additional data loss.
5. Document **everything** known about the breach.

## Follow the plan.

6. Interview those involved in discovering the breach and anyone else who may know about it.
7. Consider notifying law enforcement after consulting with legal counsel.
8. Revisit state and federal regulations governing your industry and the type of data lost.
9. Determine all persons/entities that need to be notified, i.e. customers, employees, the media,
10. Ensure all notifications occur within any mandated timeframes.

The background of the slide is a vibrant green bokeh effect, consisting of numerous out-of-focus light spots of varying sizes and intensities, creating a sense of depth and movement. The colors range from bright, almost white-green to deep, dark teal and blue-green.

# NOTICE REQUIREMENTS

# NOTICE REQUIREMENTS



- **Factors that decreased and increased the cost of a data breach.** Having a strong security posture, incident response plan and CISO appointment reduced the cost per record by \$14.14, \$12.77 and \$6.59, respectively. Factors that increased the cost were those that were caused by lost or stolen devices (+ \$16.10), third party involvement in the breach (+ \$14.80), quick notification (+ \$10.45) and engagement of consultants (+ \$2.10).

Source:  
Ponemon Institute LLC  
**Cost of Data Breach Study:  
Global Analysis**  
(May 2014)



# NOTICE REQUIREMENTS

- Different Types of Notice
  - Industry-Specific, e.g. HIPAA / HITECH
  - 47 Different State Notification Laws
    - e.g., Pennsylvania
  - Business Partners
    - e.g., New Jersey
  - Others, e.g., Regulators, AGs, Consumer Reporting Agencies, Law Enforcement?
  - Media
  - Social Media
  - SEC Filings

# NOTICE REQUIREMENTS

- Industry-Specific, e.g. HIPAA / HITECH, GLB

45 C.F.R. § 164.404

(a) Standard--

(1) General rule. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) Breaches treated as discovered. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

(b) Implementation specification: Timeliness of notification. Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

# NOTICE REQUIREMENTS

- 47 different state notification laws, e.g., Pennsylvania

## § 2303. General rule.

**(a) General rule.**--An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 [FN1] or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.

**§ 2308. Civil relief.** A violation of this act shall be deemed to be an unfair or deceptive act or practice in violation of the act of December 17, 1968 (P.L. 1224, No. 387), known as the Unfair Trade Practices and Consumer Protection Law. The Office of Attorney General shall have exclusive authority to bring an action under the Unfair Trade Practices and Consumer Protection Law for a violation of this act.

# NOTICE REQUIREMENTS

- Business Partners, e.g., New Jersey

N.J.S.A. 56:8-163

Any business or public entity that compiles or maintains computerized records that include personal information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers, as provided in subsection a. of this section, of any breach of security of the computerized records **immediately following discovery**, if the personal information was, or is reasonably believed to have been, accessed by an unauthorized person.

# NOTICE REQUIREMENTS

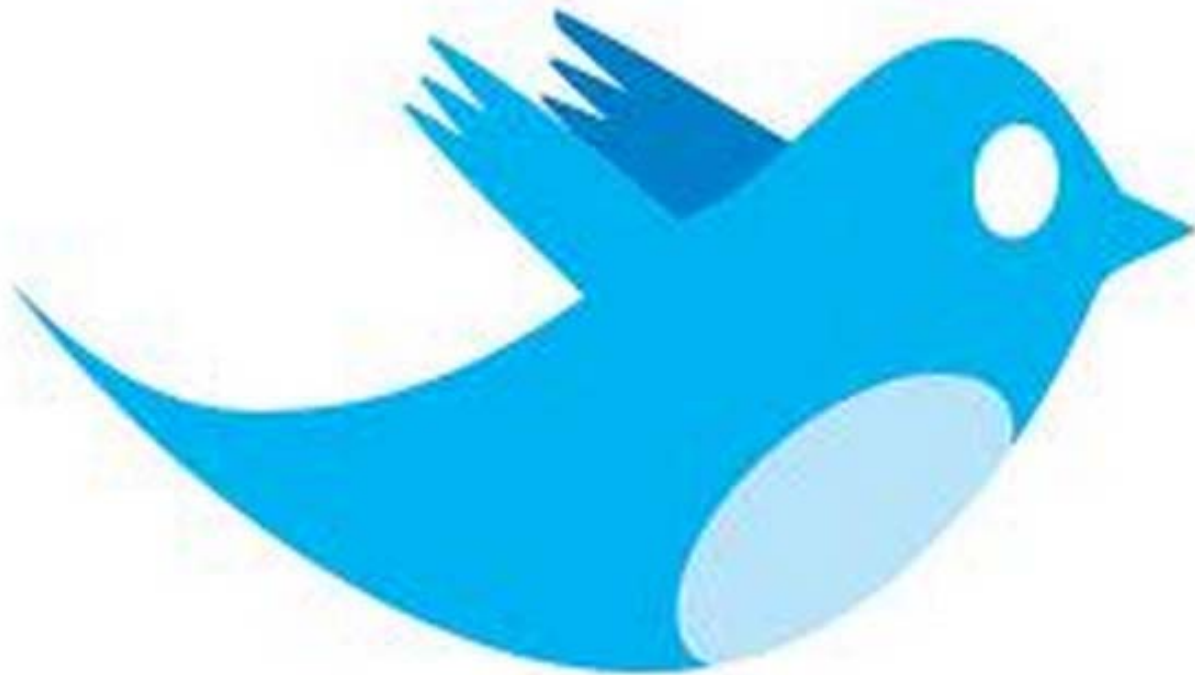




# NOTICE REQUIREMENTS



# NOTICE REQUIREMENTS



## NOTICE REQUIREMENTS

We note your disclosure that an unauthorized party was able to gain access to your computer network “in a prior fiscal year.” So that an investor is better able to understand the materiality of this cybersecurity incident, please revise your disclosure to identify when the cyber incident occurred and describe any material costs or consequences to you as a result of the incident. **Please also further describe your cyber security insurance policy, including any material limits on coverage.**

- Alion Science and Technology Corp. S-1 filing (March 2014)



# Theories of Injury Raised by Consumers and Financial Institutions in Response to Data Breaches

## CATEGORIES OF PLAINTIFFS ALLEGING DATA BREACH RELATED CLASS CLAIMS

- Class action litigation following in the wake of cyber-security data breaches are generally brought by one of two groups of plaintiffs:
  - Consumers, alleging that their personal financial information has been stolen or compromised, or is at risk of being stolen or compromised, as a result of the purported data breach and defendants' purported failure to adequately safeguard consumers' personal and financial information; and
  - Financial Credit Institutions, that issue payment cards, including debit cards and credit cards, alleging injury related to the costs incurred to protect card holders from identity theft and to reimburse card holders for losses arising from the purported data breach.
- The majority of putative class actions to date have been filed by Consumer Plaintiffs.
  - Both groups of plaintiffs, however, generally allege injury based on defendants' purported failure to adequately protect consumers' personal and financial information and defendants' purported failure to implement sufficient cyber-security procedures and measures to protect such information.



# THEORIES OF INJURY ALLEGED BY CONSUMER PLAINTIFFS

- Putative Class Action Complaints filed by Consumer Plaintiffs generally allege the following types of injury and damages:
  - Fraudulent Charges: Unauthorized charges and fees on debit and credit card accounts, and other charges and fees associated with data breach (*i.e.*, new card and late fees);
  - Identity Theft: Theft and potential sale of consumer personal and financial information;
  - Monitoring Accounts: Costs of monitoring, detecting, preventing, and attempting to mitigate possible identity theft and unauthorized use of Consumer Plaintiffs' financial accounts;
  - Future Risk of Charges/Theft: Increased risk to Consumer Plaintiffs' personal and financial information of identity theft and potential future data breaches;
  - Loss of Use & Access to Accounts: Inability to use or access accounts and costs associated with limited or restricted access to accounts, including inability to pay other bills;
  - Loss of Time, Opportunity Costs, & Stress: Loss of time and stress, anxiety, and nuisance of addressing and attempting to mitigate actual and potential future loss from the data breach;
  - Decreased Value of Personal Financial Information: Reduced value of personal and financial information as a result of its potential exposure to the public; and
  - Cost of and Overpayment for Product: Consumer Plaintiff would not have purchased a product had he or she known of allegedly deficient cyber-security practices, or overpaid for the product in light of the failure to safeguard personal and financial information (this assumes the price of products include the cost of securing consumer information).

## EXAMPLES OF CLASS ACTION LITIGATION FILED BY CONSUMER PLAINTIFFS

- *In re Barnes & Noble Pin Pad Litig.*, No. 1:12-CV-08617 (N.D. Ill.) (motion to dismiss original complaint granted; motion to dismiss amended complaint pending)
- *Moyer v. Michaels Stores, Inc.*, No. 1:14-cv-00561 (N.D. Ill.) (court granted defendant's motion to dismiss and dismissed claims in July 2014)
- *In re: Target Corp. Customer Data Security Breach Litig.*, No. 0:14-md-02522-PAM (D. Minn.) (court denied motion to dismiss; case remains pending)
- *In re: The Home Depot, Inc., Customer Data Security Breach Litig.*, No. 1:14-md-02583-TWT (N.D. Ga.) (case is pending; early stages of litigation; no motion to dismiss practice yet)
- *In re Sony Gaming Networks and Customer Data Security Breach Litig.*, No. 3:11-md-02258-AJB-MDD (S.D. Cal.) (seeking court approval for settlement of Consumer Plaintiffs' claims on a class basis)
- *In re LinkedIn User Privacy Litigation*, No. 5:12-cv-03088-EJD (N.D. Cal.) (seeking preliminary approval of class settlement of Consumer Plaintiffs' claims)
- *In re Hannaford Bros. Co. Customer Data Security Breach Litigation*, No. 2:08-md-01954-DBH (D. Me.) (after denial of motion for class certification, Consumer Plaintiffs' claims settled on individual bases)

## EXAMPLES OF CLASS ACTION LITIGATION FILED BY CONSUMER PLAINTIFFS

- *In re TJX Cos. Retail Security Breach Litig.*, No. 1:07-cv-10162-WGY (D. Mass.) (after denial of motion for class certification, Financial Institution Plaintiffs' claims settled on an individual basis)
- *Galaria v. Nationwide Mutual Ins. Co.*, Nos. 2:13-cv-118, 2:13-cv-257 (S.D. Ohio) (motion to dismiss granted for lack of Article III Standing)
- *In re Adobe Systems, Inc. Privacy Litig.*, No. 13-cv-05226-LHK (N.D. Cal.) (court granted in part and denied in part motion to dismiss; the parties are in the pre-class certification discovery stage)
- *In re: Science Applications International Corp. (SAIC) Backup Tape Data Theft Litig.*, No. 12-347 (JEB), MDL No. 2360 (D.D.C.) (court granted in part and denied in part motion to dismiss, permitted the filing of a supplemental consolidated amended complaint, and granted defendant leave to file a partial motion to dismiss the amended complaint);
- *Corona v. Sony Pictures Entertainment, Inc.*, No. 2:14-cv-09600-RGK-SH (C.D. Cal.) (several recently-filed putative class actions filed by employees or former employees of Sony arising from Sony's recent data breach have been consolidated before one U.S. District Judge; cases are in the pleadings stage)

## THEORIES OF INJURY ALLEGED BY FINANCIAL INSTITUTION PLAINTIFFS

- Putative Class Action Complaints filed by Financial Institution Plaintiffs generally allege the following types of injury and damages:
  - Notice: Costs of notifying bank account, credit card, or debit card customers of the data breach and potential for identity theft;
  - Reissuance of Cards: Costs of reissuing credit cards or debit cards to consumers potentially affected by the data breach;
  - Reimbursement: Costs of reimbursing customers for actual fraudulent transactions and charges resulting from the data breach;
  - Fraud Monitoring: Costs of increased monitoring of customer accounts to detect and prevent fraudulent charges, fees, and transactions;
  - Customer Complaints: Costs of communicating with customers and addressing increased customer complaints resulting from or related to the data breach;
  - Changing/Cancelling Accounts: Costs of changing or cancelling customer bank, credit card, or debit card accounts;
  - Lost Revenue: Loss of interest, transaction fees, and other charges and fees associated with the decrease or suspension of cardholders use of affected debit and credit cards following the data breach; and
  - Lost Customers: Loss of customers who cancelled accounts.

## EXAMPLES OF CLASS ACTION LITIGATION FILED BY FINANCIAL INSTITUTION PLAINTIFFS

- *In re: Target Corp. Customer Data Security Breach Litig.*, No. 0:14-md-02522-PAM (D. Minn.)
  - The *Target* Multi-District Litigation (“MDL”) proceeding includes putative class action complaints filed by Consumer Plaintiffs and a consolidated class action complaint filed by Financial Institution Plaintiffs.
  - Financial Institution Plaintiffs include five state- or federally-chartered banks and savings associations:
    - Umpqua Bank (Oregon state-chartered commercial bank)
    - Mutual Bank (Massachusetts state-charted mutual bank)
    - Village Bank (Minnesota state-chartered, family-owned, community bank)
    - CSE Federal Credit Union (federally-chartered, member-owned cooperative bank based in Louisiana)
    - First Federal Savings (federally-charted savings association headquartered in Ohio).



## EXAMPLES OF CLASS ACTION LITIGATION FILED BY FINANCIAL INSTITUTION PLAINTIFFS, CONT'D

- *In re: The Home Depot, Inc., Customer Data Security Breach Litigation*, No. 1:14-md-02583-TWT (N.D. Ga.)
  - The *Home Depot* MDL also includes putative class action complaints filed by Consumer Plaintiffs and Financial Institution Plaintiffs.
- Financial Institution Plaintiffs include:
  - First Choice Federal Credit Union (federally-chartered credit union from Pennsylvania)
  - Firefighters Credit Union (federally-chartered credit union from Wisconsin)
  - Animas Credit Union (New Mexico-chartered credit union)
  - KC Police Credit Union (Kansas-based credit union)
  - Suncoast Credit Union (Florida-based credit union)
  - Cattaraugus County School Employees Federal Credit Union (not-for-profit, member-owned, financial cooperative from New York)
  - Salisbury Bank and Trust Company (federally-chartered community bank in Connecticut)
  - Amalgamated Bank (New York-based banking institution)
  - Profinium, Inc. (a Minnesota corporation that provides credit and debit cards)
  - Savings Institute Bank and Trust Company (federally-chartered community bank in Connecticut)



# Statutory and Common Law Causes of Action Typically Pleaded by Plaintiffs

## CONSUMER PLAINTIFFS' TYPICAL CAUSES OF ACTION, COMMON LAW CLAIMS

- **Breach of Express Contract:**
  - Alleging breach of express contractual agreements entered into between Consumer Plaintiffs and Defendants, typically alleged through Defendant-specific privacy policies or disclosures or Defendant-specific credit or debt card agreements with consumers (*e.g.*, the Target RedCard debit card agreement).
  - Alleging express contracts promised protection of Consumer Plaintiffs' personal and financial information from unauthorized access and unauthorized use.
- **Breach of Implied Contract:**
  - Alleging that Consumer Plaintiffs entered into implied contracts with Defendants when they provided personal and financial information to Defendants to purchase products.
  - Alleging that implied contracts obligated Defendants to adequately and reasonably safeguard and protect Consumer Plaintiffs' personal and financial information and to timely and accurately notify them when their data was potentially breached.
- **Breach of Warranty (Express & Implied):**
  - Alleging that Defendants' promises and representations regarding their products and their cyber-security policies and practices created express or implied warranties to Consumer Plaintiffs that their personal and financial information would be protected.
  - Alleging that Consumer Plaintiffs would not have purchased products from Defendant or overpaid for products as a result of Defendants' breach of warranty by failing to provide adequate cyber-security measures to protect Consumer Plaintiffs' information.

## CONSUMER PLAINTIFFS' TYPICAL CAUSES OF ACTION, COMMON LAW CLAIMS, CONT'D

- Negligence:
  - Alleging that Defendants owed a duty to Consumer Plaintiffs to: (1) exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting personal and financial information from being lost, stolen, compromised, accessed, or misused; (2) design, maintain, and test their cyber-security systems to ensure that Consumer Plaintiffs' personal and financial information was reasonably secured and protected; (3) ensure that the security systems were consistent with industry standards; and (4) implement processes to timely detect, address, and disclose data breaches to Consumer Plaintiffs.
- Negligent Misrepresentation:
  - Alleging that Defendants' actions and statements misrepresented the character, quality, and adequacy of their cyber-security policies, procedures, and practices or Defendants failed to disclose the alleged inadequacy of their cyber-security procedures.
  - Alleging that Consumer Plaintiffs would not have purchased or would not have paid the price that they did for the products had they known of the alleged inadequacy of the Defendants' security measures.
- Breach of Fiduciary Duty:
  - Alleging that Defendants breached their fiduciary duties to Consumer Plaintiffs by failing to adequately safeguard their personal and financial information.

## CONSUMER PLAINTIFFS' TYPICAL CAUSES OF ACTION, COMMON LAW CLAIMS, CONT'D

- Unjust Enrichment:
  - Alleging that Consumer Plaintiffs conferred a benefit on Defendants by paying money to purchase goods or products, which payment included costs for the provision of reasonable cyber and personal and financial data security to Consumer Plaintiffs.
  - Alleging that Defendants' failure to provide reasonable and adequate cyber-security measures and to protect Consumer Plaintiffs' personal and financial information caused Plaintiffs to either purchase products they would not have purchased or to overpay for such products.



## CONSUMER PLAINTIFFS' TYPICAL CAUSES OF ACTION, STATUTORY CLAIMS

- Violation of State Consumer Protection/Unfair and Deceptive Trade Practices Act Statutes (“UDAP”)
  - Consumer Plaintiffs generally allege that Defendants’ alleged failures to (1) implement adequate, reasonable cyber-security measures to protect against data breaches, (2) implement cyber-security measures consistent with industry standards, (3) disclose their allegedly inadequate security measures, or (4) timely notify Consumer Plaintiffs of a data breach, constitute unfair, fraudulent, or deceptive conduct under state UDAP statutes.
  - State UDAP statutes often provide for the recovery of actual damages, double or treble damages, punitive damages, or attorneys’ fees by a successful Plaintiff.
- Violation of State Data-Breach Notification Statutes
  - More than 30 states have statutes that govern or create obligations regarding timely and accurate disclosure of a data breach by a Defendant.
  - Consumer Plaintiffs have asserted claims alleging that Defendants failed to timely or accurately disclose data breaches, leaving Consumer Plaintiffs’ unable, or less able, to protect their personal and financial information prior to disclosure.
- Violation of State Privacy and Data Disclosure Laws
  - State-specific claims regarding Defendants’ alleged handling of Consumer Plaintiffs’ personal and financial information and the disclosure of personal or private consumer information.

## CONSUMER PLAINTIFFS' TYPICAL CAUSES OF ACTION, STATUTORY CLAIMS, CONT'D

- Violation of the Federal Stored Communications Act, 18 U.S.C. §§ 2702, *et seq.* (“FSCA”)
  - Alleging that Defendants provided “electronic communications services” or “remote computing services” by providing for credit and debit card payment processing services and that Defendants’ alleged failure to implement reasonable cyber-security measures permitted the “knowing” dissemination of Consumer Plaintiffs’ personal and financial information.
  - At least one court has dismissed claims under the FSCA against a retail defendant on the grounds that the defendant did not provide “electronic communications services” or “remote computing services” as defined by the FSCA. *See In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 523-24 (N.D. Ill. 2011).
- Violation of the Fair Credit Reporting Act, 15 U.S.C. §§ 1681, *et seq.* (“FCRA”)
  - Alleging that Defendants were “credit reporting agencies” and that they were under a statutory duty to adopt and maintain procedures to protect against the dissemination, disclosure, or theft of consumer credit and other financial information under FCRA.
  - Courts have dismissed FCRA claims against data breach defendants on the grounds that many data breach defendants are not “consumer reporting agencies” and are not subject to liability under its provisions. *See, e.g., In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1010-12 (S.D. Cal. 2014).

## FINANCIAL INSTITUTION PLAINTIFFS' TYPICAL CAUSES OF ACTION, COMMON LAW CLAIMS

- Negligence:
  - Alleging that Defendants owed duties of care to Financial Institution Plaintiffs: (1) to exercise reasonable care in obtaining, retaining, securing, using, and deleting the personal and financial information of customers who used credit or debit cards to purchase products from them; (2) to provide cyber-security measures consistent with industry standards and requirements; (3) to ensure that consumer information is adequately protected; and (4) to comply with state and federal laws governing disclosure of consumer information or credit and debit card transactions.
- Negligent Misrepresentation by Omission:
  - Alleging that Defendants, through their privacy policies and other actions and representations, failed to disclose or negligently omitted:
    - (1) that they had inadequate cyber-security policies and practices to protect consumers personal and financial information;
    - (2) that they did not comply with security standards set forth in (a) Card Operating Regulations issued by debit and credit card companies, and (b) the Payment Card Industry Data Security Standards issued by the Payment Card Industry Security Standards Council; and
    - (3) timely and accurate information regarding data breaches to consumers and Financial Institution Plaintiffs after they had knowledge of the breaches.

## FINANCIAL INSTITUTION PLAINTIFFS' TYPICAL CAUSES OF ACTION, STATUTORY CLAIMS

- Violation of State Law Applicable to Credit or Debit Card Transactions.
  - *E.g.*, Minnesota Plastic Card Security Act (Minn. Stat. § 325E.64) (alleged in Target Financial Institution Plaintiffs' Consolidated Complaint).
- Negligence *Per Se* Claims Based on Alleged Statutory Violations:
  - Several Complaints filed by Financial Institution Plaintiffs against The Home Depot have alleged Negligence *Per Se* common law claims based on alleged violations of the federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801, *et seq.*).
  - The Financial Institution Plaintiffs in the Target MDL have alleged a Negligence *Per Se* claim against Target based on its alleged violation of the Minnesota Plastic Card Security Act (Minn. Stat. § 325E.64).

## POTENTIAL CAUSES OF ACTION FOR INDEMNIFICATION BY DEFENDANTS

- Defendants may have potential claims for indemnification against third-parties to recover some, or all, financial losses associated with a breach.
- Potential third-parties may include:
  - Service providers;
  - Technology suppliers;
  - Other third-parties involved in setting up or maintaining electronic payment systems; or
  - Insurance companies.
- Potential causes of action may include:
  - Negligence;
  - Negligent misrepresentation;
  - Breach of contract;
  - Violation of State UDAP statutes and other State statutory claims.
- There are few reported cases addressing data-breach indemnification claims.
  - See *Cotton Patch Cafe, Inc. v. Micros Sys., Inc.*, No. MJG-09-03242, 2012 WL 5986773 (D. Md. Nov. 27, 2012) (granting summary judgment on some indemnification-based claims arising from data breach)
- Indemnification suits may follow in the wake of large-scale, high-profile data breach litigation matters, such as those pending against Target, Home Depot, and Sony.





# Approaches to Defending Data Breach Claims and Opposing Class Certification

## PROCEDURAL CONSIDERATIONS: JURISDICTION, FEDERAL OR STATE COURT

- Federal Court: The majority of data-breach class action complaints are filed in the United States District Courts.
  - Data breaches often impact plaintiffs in multiple states such that a putative class action could potentially be filed in several different federal district courts.
- State Court: Where a data-breach class action is filed in state court, a defendant should consider removal to federal court.
  - Federal Question Jurisdiction: Does the complaint assert a cause of action under a federal statute or do state law claims substantially depend or rely on the interpretation of federal law?
  - Diversity Jurisdiction Under the Class Action Fairness Act (“CAFA”):
    - Does the putative class include more than 100 potential class members?
    - Does minimal diversity exist between the named plaintiffs and the named defendants?
    - Does the amount-in-controversy for the putative class claims exceed \$5 million?
  - In the majority of data-breach class actions, the putative class size and amount-in-controversy requirements are met based on the allegations in the complaint.
  - Minimal diversity will normally be present, unless the complaint was filed by a plaintiff that resides in the same jurisdiction in which the defendant resides (*i.e.*, where it is incorporated or has its principal place of business).

## PROCEDURAL CONSIDERATIONS: MULTI-DISTRICT LITIGATION / CONSOLIDATION

- In the wake of most cyber-security/data breaches, defendants will face multiple putative class actions filed in several different state and federal courts.
- This raises the following procedural considerations for a defendant:
  - Consolidation: Consolidation of pending cases filed in the same federal district court or state court before one judge.
  - Multi-District Litigation (“MDL”): Transfer to and consolidation of all related federal cases, filed in multiple federal district courts, before one federal district judge for all pre-trial proceedings, including motions to dismiss, discovery, class certification, and related proceedings.
- Most data-breach class actions are consolidated or transferred to an MDL proceeding, often, but not always, located in the federal district court in the jurisdiction in which the defendant has its principal place of business.

## PROCEDURAL CONSIDERATIONS: MULTI-DISTRICT LITIGATION / CONSOLIDATION

- Benefits of Consolidation or MDL Proceedings:
  - Avoids duplicative motion practice, discovery, and other pre-trial proceedings across potentially hundreds of substantially-similar cases in multiple jurisdictions.
  - Avoids inconsistent pre-trial rulings by different courts.
  - Reduces costs and expenses associated with separately litigating substantially-similar cases in multiple jurisdictions.
  - Promotes global settlement discussions.
- Disadvantages of Consolidation or MDL Proceedings:
  - Risk of assignment to an unfavorable jurisdiction or district court judge.
  - MDL proceedings are often slow and frequently bogged down with procedural issues.
  - Risk that weak and deficiently pleaded cases are permitted to advance to discovery based on the relative strength of better pleaded complaints.
  - Permits multiple plaintiffs' attorneys to combine and marshal their resources and experience.

## THE PLEADING STAGE: MOTIONS TO DISMISS

- In defending data breach class actions, defendants in most cases have initially moved to dismiss the named plaintiffs' claims.
- The most common arguments in support of motions to dismiss include:
  - Lack of Article III Standing – particularly the failure to allege facts supporting the existence of an “injury-in-fact”;
  - Failure to State a Claim for Relief under Rule 12(b)(6)
    - Failure to sufficiently allege ascertainable loss, injury, or harm;
    - Failure to sufficiently allege the elements of each claim;
    - Failure to sufficiently allege a right to recovery under statutory claims; and
    - Dismissal of certain claims as a matter of law (*i.e.*, named plaintiffs cannot state a claim for relief under a specific cause of action).
- Defendants have obtained mixed results on motions to dismiss in data breach actions.

## THE PLEADING STAGE: MOTIONS TO DISMISS

- Examples of Successful Motions to Dismiss:
  - Lewert v. P.F. Chang's China Bistro, Inc., No. 14-cv-4787, 2014 WL 705097 (N.D. Ill. Dec. 10, 2014) (dismissing Consumer Plaintiffs' claims for lack of standing);
  - Remijas v. The Neiman Marcus Group, LLC, No. 14 C 1735, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014) (dismissing Consumer Plaintiffs' claims for lack of standing);
  - Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014) (finding standing, but dismissing Consumer Plaintiffs' claims for failure to state claims based on failure to plead actual economic damage);
  - Galaria v. Nationwide Mutual Ins. Co., 998 F. Supp. 2d 646 (S.D. Ohio 2014) (dismissing Consumer Plaintiffs' claims for lack of standing and failure to state claims for invasion of privacy under certain state laws);
  - In re Barnes & Noble Pin Pad Litig., No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013) (dismissing Consumer Plaintiffs' claims for lack of standing)
  - Hammer v. Sam's East, Inc., No. 12-cv-2618-CM, 2013 WL 3756573, (D. Kan. July 16, 2013) (dismissing Consumer Plaintiffs' claims for lack of standing);
  - In re LinkedIn User Privacy Litig., 932 F. Supp. 2d 1089 (N.D. Cal. 2013) (dismissing Consumer Plaintiffs' claims for lack of standing).



## THE PLEADING STAGE: MOTIONS TO DISMISS

- Examples of Mixed Results on Motions to Dismiss:
  - *In re Target Corp. Customer Data Security Breach Litig.*, MDL No. 14-2522 (PAM/JJK), 2014 WL 7192478 (D. Minn. Dec. 18, 2014) (granting in part and denying in part Consumer Plaintiffs' motion to dismiss, finding standing, but dismissing claims under certain state UDAP statutes, certain state data-breach notice statutes, and for some state law-based negligence claims);
  - *In re Target Corp. Customer Data Security Breach Litig.*, MDL No. 14-2522(PAM/JKK), 2014 WL 6775314 (D. Minn. Dec. 2, 2014) (granting in part and denying in part Financial Institution Plaintiffs' motion to dismiss, which dismissed negligent misrepresentation claim without prejudice);
  - *In re Sony Gaming Networks and Customer Data Security Breach Litig.*, 966 F. Supp. 2d 942 (S.D. Cal. 2014) (finding Consumer Plaintiffs had standing, but granting in part and denying in part motion to dismiss for failure to state a claim, dismissing most of plaintiffs' state law claims for negligence, negligent misrepresentation, breach of warranty, and unjust enrichment, and dismissing claims alleging violation of certain state UDAP statutes); and
  - *In re: Michaels Stores Pin Pad Litig.*, 839 F. Supp. 2d 518 (N.D. Ill. 2011) (dismissing claims for violation of the Federal Stored Communications Act, negligence, negligence *per se*, and portions of Illinois state UDAP claims).

## THE PLEADING STAGE: MOTIONS TO DISMISS FOR LACK OF STANDING

- Article III Standing is often one of the most common arguments that a data-breach defendant may assert in a motion to dismiss.
- To have Article III Standing, a named plaintiff must plead fact-based allegations that demonstrate that:
  - He or she has suffered an “injury-in-fact” that is actual, concrete, and particularized;
  - The injury-in-fact is fairly traceable to the defendants’ alleged conduct; and
  - The injury-in-fact can be redressed by a favorable decision.
- Where a named plaintiff alleges potential future injury that he or she may suffer, the alleged injury must be imminent and “certainly impending” to support Article III Standing.
  - See *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138, 1147 (2013) (“we have repeatedly reiterated that threatened injury must be certainly impending to constitute injury in fact, and that allegations of possible future injury are not sufficient” (internal quotation marks omitted)).

## THE PLEADING STAGE: MOTIONS TO DISMISS FOR LACK OF STANDING

- Courts have dismissed Consumer Plaintiffs' claims for lack of Standing for a failure to plausibly allege "injury-in-fact" where:
  - Named plaintiffs have not alleged that their personal and financial information was actually stolen or used, or that they suffered specific fraudulent charges or theft of their funds or identity;
    - Complaints often lack these basic allegations of injury. That information may have been stolen is not enough to support Standing.
  - Plaintiffs' claims are based on a risk of future injury that is not "certainly impending;"
    - Increased risk of identity theft or fraudulent charges; and
    - Costs of mitigation efforts to prevent future identity theft (mitigation expenses do not qualify as actual injuries when the harm sought to be prevented is not itself imminent).
  - Plaintiffs' theories of injury do not state a plausible injury-in-fact:
    - Overpayment for products;
    - Opportunity costs and loss of ability to use debit or credit cards; and
    - Alleged diminution of value of named plaintiffs' personal information.

## THE PLEADING STAGE: MOTIONS TO DISMISS FOR LACK OF STANDING

- On the other hand, Courts have found that named plaintiffs have Article III Standing to bring data-breach related claims where they plead specific allegations demonstrating:
  - That their personal and financial information has actually been stolen or they have suffered actual identity theft;
  - That they have suffered actual fraudulent charges, fees, or other costs on their debit or credit card accounts; and
  - That they have had restricted or blocked access to bank accounts.
- Courts have also found Article III Standing for the alleged increased risk of future harm based on a narrower interpretation of the Supreme Court's decision in Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1147 (2013).
  - Courts dismissing data-breach claims have generally relied on Clapper as establishing a high Standing threshold for alleging potential, future risks of injury for only those injuries that are "certainly impending."
  - Courts finding Article III Standing for alleged future harm have generally interpreted Clapper narrowly to apply only to the unique facts at issue in that case and, relying on pre-Clapper case law, have found that the risk that named plaintiffs' personal and financial information will be misused by hackers after a data breach is sufficiently immediate and real to establish Article III Standing.

## THE PLEADING STAGE: MOTIONS TO DISMISS FOR LACK OF STANDING, POST-CLAPPER EXAMPLES

- Cases Dismissed for Lack of Article III Standing under *Clapper*
  - *Lewert v. P.F. Chang's China Bistro, Inc.*, No. 14-cv-4787, 2014 WL 705097 (N.D. Ill. Dec. 10, 2014) (dismissing Consumer Plaintiffs' claims for lack of standing);
  - *Remijas v. The Neiman Marcus Group, LLC*, No. 14 C 1735, 2014 WL 4627893 (N.D. Ill. Sept. 16, 2014) (dismissing Consumer Plaintiffs' claims for lack of standing);
  - *Galaria v. Nationwide Mutual Ins. Co.*, 998 F. Supp. 2d 646 (S.D. Ohio 2014) (dismissing Consumer Plaintiffs' claims for lack of standing and failure to state claims for invasion of privacy under certain state laws);
  - *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588 (N.D. Ill. Sept. 3, 2013) (dismissing Consumer Plaintiffs' claims for lack of standing)
  - *Hammer v. Sam's East, Inc.*, No. 12-cv-2618-CM, 2013 WL 3756573, (D. Kan. July 16, 2013) (dismissing Consumer Plaintiffs' claims for lack of standing);
  - *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089 (N.D. Cal. 2013) (dismissing Consumer Plaintiffs' claims for lack of standing)
  - *In re Science Applications International Corp. (SAIC) Backup Data Theft Litig.*, No. 12-347 (JEB), 2014 WL 1858458 (D.D.C. May 9, 2014) (dismissing most Consumer Plaintiffs' claims for lack of standing; finding standing as to only two plaintiffs – one who alleged actual misuse of financial information, and one who alleged privacy violations linked to personal medical information)

## THE PLEADING STAGE: MOTIONS TO DISMISS FOR LACK OF STANDING, POST-CLAPPER EXAMPLES

- Cases Finding Article III Standing after *Clapper*
  - *In re Target Corp. Customer Data Security Breach Litig.*, MDL No. 14-2522 (PAM/JJK), 2014 WL 7192478 (D. Minn. Dec. 18, 2014) (holding that Consumer Plaintiffs had standing; the court did not discuss or cite to *Clapper*)
  - *In re Adobe Systems, Inc. Privacy Litig.*, No. 13-cv-05226-LHK, 2014 WL 4379916 (N.D. Cal. Sept. 9, 2014) (finding that Consumer Plaintiffs had standing to assert certain of their California state law claims)
  - *Moyer v. Michaels Stores, Inc.*, No. 14 C 561, 2014 WL 3511500 (N.D. Ill. July 14, 2014) (finding standing, but dismissing Consumer Plaintiffs' claims for failure to state claims based on failure to plead actual economic damage)
  - *In re Sony Gaming Networks and Customer Data Security Breach Litig.*, 966 F. Supp. 2d 942 (S.D. Cal. 2014) (finding that Consumer Plaintiffs had standing to assert data-breach based claims based on "credible threat" of impending harm based on disclosure of personal and financial information)
  - *In re Zappos.com, Inc.*, No. 3:12-cv-00325-RCJ-VPC, 2013 WL 4830497 (D. Nev. Sept. 9, 2013) (finding Consumer Plaintiffs had standing based on increased risk of fraud and costs of monitoring credit scores and securing financial information)



## THE PLEADING STAGE: MOTIONS TO DISMISS FOR LACK OF STANDING

- Article III Standing Conclusions for Consumer Plaintiffs' Claims:
  - Success will likely depend on the thoroughness and specificity of the claims and allegations of injury pleaded in the complaint; and
  - The Court's interpretation and application of the Supreme Court's Clapper decision to allegations of potential future harm.
- Article III Standing arguments are less applicable to Financial Institution Plaintiffs' claims.
  - Financial Institution Plaintiffs' claims are ordinarily based on allegations of actual past injuries from specific costs and expenses incurred by Plaintiffs in the wake of a data breach.
- Summary Judgment: If unsuccessful on a motion to dismiss, a Defendant may raise Standing and other injury-in-fact arguments in a motion for summary judgment on the named plaintiffs' individual claims.
  - See Kahle v. Litton Loan Servicing LP, 486 F. Supp. 2d 705 (S.D. Ohio. 2007) (granting summary judgment based on Consumer Plaintiff's failure to establish actual and imminent injury; personal information was not accessed, no identity fraud was proven, and purchase of credit monitoring alone was insufficient to establish injury)

## THE PLEADING STAGE: MOTIONS TO DISMISS FOR FAILURE TO STATE A CLAIM FOR RELIEF

- Defendants may also seek dismissal of data breach claims based on the named plaintiffs' failure to state a claim upon which relief can be granted under Rule 12(b)(6).
- Failure to State a Claim arguments are generally cause of action specific and turn on:
  - The elements required to plead a plausible cause of action;
  - Whether the basic pleading standard (Rule 8) or a heightened pleading standard for fraud-based claims (Rule 9(b)) applies to the specific cause of action; or
  - The state law applicable to that cause of action.

## THE PLEADING STAGE: MOTIONS TO DISMISS FOR FAILURE TO STATE A CLAIM FOR RELIEF

- Arguments attacking a named plaintiffs' failure to plausibly allege each element of their causes of action have included:
  - Failure to plausibly allege injury, ascertainable loss, or damage (for causes of action where actual harm or actual damages are required to establish a claim for relief);
  - Failure to plausibly allege causation – *i.e.*, that any alleged loss, injury, or damages were actually and proximately caused by the alleged data breach;
  - Failure to plausibly allege fraud-based claims with specificity under Fed. R. Civ. P. 9(b) (this argument would apply to fraud, misrepresentation, and certain state UDAP claims); and
  - Failure to plausibly allege the existence of a contract or warranty on which to base breach of contract and breach of warranty claims.

## THE PLEADING STAGE: MOTIONS TO DISMISS FOR FAILURE TO STATE A CLAIM FOR RELIEF

- Arguments attacking a named plaintiffs' inability, as a matter of law, to state a claim for certain data breach causes of action have included:
  - Economic Loss Doctrine: The Economic Loss Doctrine may bar plaintiffs from asserting tort claims, such as negligence, under some states' laws where plaintiffs do not allege that they suffered personal injury or property damage;
    - *In re Target Corp. Customer Data Security Breach Litig.*, MDL No. 14-2522 (PAM/JJK), 2014 WL 7192478 (D. Minn. Dec. 18, 2014) (dismissing Consumer Plaintiffs' negligence claims pursuant to the Economic Loss Doctrine under Alaska, California, Illinois, Iowa, and Massachusetts law).
  - No Private Right of Action: Some state statutes may not provide for a private cause of action for private plaintiffs to enforce the statute;
    - State data-breach notice statutes in some states.
    - State UDAP statutes in some states limit the circumstances in which a private plaintiff may assert statutory claims.
  - Statutory Defenses: State statutory defenses may preclude data-breach claims.
  - Class Action Prohibition: Some state statutes expressly prohibit a plaintiff from pursuing class action claims.

## THE PLEADING STAGE: MOTIONS TO DISMISS FOR FAILURE TO STATE A CLAIM FOR RELIEF

- Defendants may argue that some claims are not applicable to defendants or to data-breach cases:
  - Violation of the Federal Stored Communications Act, 18 U.S.C. §§ 2702, *et seq.* (“FSCA”).
    - At least one court has dismissed data-breach related claims under the FSCA against a retailer defendant on the grounds that the defendant did not provide “electronic communications services” or “remote computing services” as defined by the FSCA. *See In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 523-24 (N.D. Ill. 2011).
  - Violation of the Fair Credit Reporting Act, 15 U.S.C. §§ 1681, *et seq.* (“FCRA”)
    - Courts have dismissed FCRA claims against data-breach defendants on the grounds that many defendants are not “consumer reporting agencies” and are not subject to liability under FCRA. *See, e.g., In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942, 1010-12 (S.D. Cal. 2014).

## MOTIONS FOR SUMMARY JUDGMENT ON NAMED PLAINTIFFS' CLAIMS

- Defendant may raise similar arguments to those made in a motion to dismiss, including standing and injury/damage based arguments, in a motion for summary judgment on the named plaintiffs' individual claims.
  - See, e.g., Kahle v. Litton Loan Servicing LP, 486 F. Supp. 2d 705 (S.D. Ohio. 2007)
  - The Court granted summary judgment based on Consumer Plaintiff's failure to establish actual and imminent injury, finding that: (1) plaintiff's personal information was not accessed as a result of the data breach; (2) she failed to present any evidence of identity fraud; and (3) the purchase of credit monitoring alone was insufficient to establish actionable injury or damages to support negligence claims.
- A motion for summary judgment may be filed in connection with an opposition to a motion for class certification as a means to:
  - Obtain judgment on plaintiffs' individual claims; and
  - Highlight individualized issues in plaintiffs' claims that may preclude class certification.



## DEFENDING AGAINST CLASS CERTIFICATION

- Fed. R. Civ. P. 23 governs whether a proposed class is appropriate for class certification.
  - Rule 23(a) Requirements for Class Certification:
    - Numerosity;
    - Commonality;
    - Typicality; and
    - Adequacy of Representation.
  - Rule 23(b) Categories of Class Actions Commonly Alleged:
    - Rule 23(b)(2): “[T]he party opposing the class has acted or refused to act on grounds that apply generally to the class, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.”
    - Rule 23(b)(3): “[T]he court finds that questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy.”

## DEFENDING AGAINST CLASS CERTIFICATION, CONT'D

- Few cases have addressed whether a putative class asserting data-breach related claims is appropriate for class certification under Rule 23.
- *In re Hannaford Bros. Co. Customer Data Security Breach Litig.*, 293 F.R.D. 21 (D. Me. 2013).
- Consumer Plaintiffs alleging claims for negligence and breach of implied contract moved to certify a proposed class defined as follows:
  - “All persons or entities . . . in the United States who made purchases at stores owned or operated by Defendant or for which Defendant provided electronic payment processing services . . . Using debit or credit cards, and who made reasonable out of pocket expenditures in mitigation of the consequences to them of an electronic breach of Defendant’s data security . . . Consisting of 1) payment of fees to obtain prompt replacement of cancelled cards and 2) purchase of security products such as credit monitoring and identity theft insurance.” *Id.* at 24.
- The Court denied Consumer Plaintiffs’ Motion for Class Certification, finding their claims inappropriate for class treatment under Rule 23(b)(3).

## DEFENDING AGAINST CLASS CERTIFICATION, CONT'D

- *In re Hannaford Bros. Co. Customer Data Security Breach Litig.*, 293 F.R.D. 21 (D. Me. 2013).
  - The Court found that the proposed class satisfied all of the requirements of Rule 23(a) and the superiority prerequisite of Rule 23(b)(3).
  - The Court, however, found that the proposed class did not satisfy the predominance requirement of Rule 23(b)(3) because individual issues of injury, causation, and damages predominated over common issues.
    - Noting individual issues of “the actual impact [of the data breach] on particular cardholders (for example, whether their particular accounts suffered fraudulent charges or not) and the actual mitigating steps they took and the costs they incurred.” *Id.* at 30.
    - “[P]laintiffs cannot prove total damages, and the alternative . . . is a trial involving individual issues for each class member as to what happened to his/her data and account, what he/she did about it, and why.” *Id.* at 33.
  - The Court suggested that expert testimony demonstrating an ability to prove total damages on a class basis might have supported certification.

## DEFENDING AGAINST CLASS CERTIFICATION, CONT'D

- *In re TJX Cos. Retail Security Breach Litig.*, 246 F.R.D. 389 (D. Mass. 2007).
- Financial Institution Plaintiffs sought to certify a class defined as:
  - “[A]ll financial institutions [nationwide] who received an alert from MasterCard or Visa related to the security breach of TJX’s computer systems . . . and identifying one or more credit or debit cards issued by the financial institution.”
- The Court denied the motion for class certification, finding that:
  - The proposed class definition was likely improper as it required “individualized fact-finding . . . to identify class members;”
  - Individualized issues of causation, reliance, injury, and damages precluded certification of negligent misrepresentation and Massachusetts UDAP claims under Rule 23(b)(3); and
  - Certification under Rule 23(b)(2) was improper because “the named plaintiffs are far more concerned with recovering the money they expended after the security breach than in obtaining equitable relief.”

## DEFENDING AGAINST CLASS CERTIFICATION, CONT'D

- All class certification defenses will depend on the specific claims, allegations, and proposed class definition pleaded by the plaintiffs.
- In light of *In re Hannaford Bros.*, *In re TJX*, and guiding principles of class certification:
  - Potential arguments in opposing class certification include:
    - Ascertainability: Membership in the proposed class, as defined, cannot be determined without conducting individualized inquiries into each putative class members' specific circumstances.
    - Insufficient Class Definition: The proposed class definition is overbroad, contains individuals who have not suffered injury, or is otherwise insufficiently pleaded.
    - Predominance / Superiority: Individual issues of injury, causation, and damages predominate over common issues, making certification under Rule 23(b)(3) inappropriate.
    - Rule 23(b)(2): Certification under Rule 23(b)(2) is likely precluded and inappropriate in most data breach class actions because the primary relief sought by data breach plaintiffs is ordinarily monetary relief.

## DEFENDING AGAINST CLASS CERTIFICATION, CONT'D

- In most data breach cases, a defendant's strongest argument will likely rest on Rule 23(b)(3)'s predominance requirement.
  - That is that individual issues necessary to adjudicate each individual putative class member's claim will predominate over issues common to the class such that putative class claims are not susceptible to class-wide resolution.
- Individual issues include:
  - Injury: Whether, how, and to what extent each putative class member allegedly suffered harm and injury (*i.e.*, the effect of the data breach on each individual putative class member).
  - Causation: Whether and how each putative class member's alleged harm was caused by the alleged data breach as opposed to intervening actions of third parties, their own actions, or other events.
  - Reliance: For claims that require a showing of reliance, whether and how each putative class member relied on alleged representations or actions of defendants.
  - Calculation of damages: The assessment of actual loss and the amount of damages suffered by each putative class member cannot be determined on a class basis, only on a member-by-member basis through individual mini-trials for each class member.



## DEFENDING AGAINST CLASS CERTIFICATION, CONT'D

- Examples of inherently individual questions of injury, causation and damages:
  - Whether each putative class member's personal and financial information was actually accessed by third-party data breachers or others;
  - Whether each putative class member's personal and financial information was actually used to make fraudulent charges;
  - Whether each putative class member was reimbursed for any fraudulent charges or whether he or she suffered loss as a result;
  - Whether each putative class member took mitigating steps to prevent against fraud before or after the breach and, if so, what specific steps were taken by each putative class member and whether those steps were reasonable;
  - Whether each putative class member was assessed fees, charges, or other costs on their accounts as a result of the data breach; and
  - The actual amount of charges, costs, fees, or other specific harm suffered by each putative class member (a question that largely depends on the answers to the other individualized questions above).
- Each of these questions requires inquiry into each putative class member's specific circumstances to determine a right to recover, injury, and damages, and cannot be determined based on common, class-wide evidence.

## DEFENDING AGAINST CLASS CERTIFICATION, CONT'D

- The U.S. Supreme Court's 2013 decision in Comcast Corp. v. Behrend, 133 S. Ct. 1426 (2013), may further strengthen data breach defendants' predominance arguments.
- In Comcast Corp., the Supreme Court held that individualized damages issues precluded certification under Rule 23(b)(3).
  - A plaintiff seeking certification of a class must "establish[ ] that damages are capable of measurement on a classwide basis." Id. at 1433.
  - Absent such a showing a plaintiff "cannot show Rule 23(b)(3) predominance: Questions of individual damage calculations will inevitably overwhelm questions common to the class." Id.
- The Comcast Corp. decision requires courts to consider individualized damages issues, like those presented in many data breach cases, in the class certification analysis.
- Comcast Corp. provides data breach defendants with a weapon with which to defend against certification of putative class actions.

## DEFENDING AGAINST CLASS CERTIFICATION, CONT'D

- To date, few courts have addressed the issue of class certification in data breach cases.
  - Some cases have been dismissed at the pleading stage;
  - Some cases have been settled prior to the class certification stage (often settled on a class basis); and
  - Some cases have not yet progressed to the class certification stage.
- Plaintiffs appear to face several obstacles to class certification that defendants can and should utilize in defending against motions for class certification in data breach class actions.
- As pending data breach cases approach the class certification stage, courts may have further opportunity to address and refine the Rule 23 class certification analysis as applied data breach cases.



# Lessons Learned from Past Data Breach Class Actions

## LESSONS LEARNED FROM PAST DATA BREACH CLASS ACTIONS

- Motions to Dismiss:
  - Defendants have had some success on motions to dismiss data-breach complaints, particularly on Article III Standing grounds as relates to Consumer Plaintiffs' claims.
  - Motions to dismiss Financial Institution Plaintiffs' claims are often more difficult to defeat at the motion to dismiss stage.
  - Success on motions to dismiss will likely depend on the specific allegations and claims pleaded in the complaint and on the specific Court/Judge hearing the motion.
- Class Certification:
  - To date, few courts have addresses the class certification in the context of data-breach class actions.
  - Class certification likely presents high hurdles for named plaintiffs' to clear to demonstrate the appropriateness of data-breach claims for class certification under Rule 23 of the Federal Rules of Civil Procedure.
  - The class certification case law may develop further in the near future as high profile data breach cases – Target & Home Depot – progress towards the class certification stage.

## LESSONS LEARNED FROM PAST DATA BREACH CLASS ACTIONS

- Settlement:
  - After defeat or partial defeat on motions to dismiss, several defendants have settled or are in the process of settling remaining data breach claims on a class-wide basis (before the Court's consideration of any motion for class certification).
    - See, e.g., *In re Sony Gaming Networks and Customer Data Security Breach Litig.*, No. 3:11-md-02258-AJB-MDD (S.D. Cal.) (court has granted preliminary approval of class settlement of Consumer Plaintiffs' claims);
    - See, e.g., *In re LinkedIn User Privacy Litig.*, No. 5:12-cv-03088-EJD (N.D. Cal.) (in the process of seeking court preliminary approval of settlement of Consumer Plaintiffs' claims on a class basis).
  - The potential size of the total class exposure, the cost of proceeding through discovery and further litigation, and other legal and business factors likely influenced defendants to settle prior to the class certification stage.



The background of the slide is an abstract, artistic composition of green and teal bokeh lights. The lights are out of focus, creating soft, glowing circles of varying sizes and intensities. The colors range from a bright, almost white-green to a deep, dark teal. The overall effect is a sense of depth and light, typical of a night scene with distant lights or a close-up of a light source through a lens.

# Insurance Coverage Considerations

# INSURANCE COVERAGE CONSIDERATIONS

- Potential Coverage Under “Legacy” Insurance Policies
- Limitations of “Legacy” Insurance Policies
- Specialized “Cyber”/Privacy Insurance Policies
- Remembering the Snowflake
- Avoiding the Traps
- Beware the Fine Print

## POTENTIAL COVERAGE UNDER “LEGACY” INSURANCE POLICIES

- Directors’ and Officers’ (D&O)
- Errors and Omissions (E&O)/Professional Liability
- Employment Practices Liability (EPL)
- Fiduciary Liability
- Crime
- Property
- Commercial General Liability (CGL)

## POTENTIAL COVERAGE UNDER “LEGACY” INSURANCE POLICIES

- Coverage B Provides Coverage for Damages Because of “Personal and Advertising Injury”
- “Personal and Advertising Injury”: “[o]ral or written publication, in any manner, of material that violates a person’s right of privacy”
  - What is a “Person’s Right of Privacy”?
  - What is a “Publication”?

# LIMITATIONS OF “LEGACY” INSURANCE POLICIES

**THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.**

## **AMENDMENT OF PERSONAL AND ADVERTISING INJURY DEFINITION**

This endorsement modifies insurance provided under the following:

COMMERCIAL GENERAL LIABILITY COVERAGE PART

With respect to **Coverage B Personal And Advertising Injury Liability**, Paragraph 14.e. of the **Definitions** section does not apply.

14. "Personal and advertising injury" means injury, including consequential "bodily injury", arising out of one or more of the following offenses:

e. Oral or written publication, in any manner, of material that violates a person's right of privacy;

# LIMITATIONS OF “LEGACY” INSURANCE POLICIES

This insurance does not apply to:

## **Access Or Disclosure Of Confidential Or Personal Information**

"Personal and advertising injury" arising out of any access to or disclosure of any person's or organization's confidential or personal information, including patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information or any other type of nonpublic information.

This exclusion applies even if damages are claimed for notification costs, credit monitoring expenses, forensic expenses, public relations expenses or any other loss, cost or expense incurred by you or others arising out of any access to or disclosure of any person's or organization's confidential or personal information.



# LIMITATIONS OF “LEGACY” INSURANCE POLICIES

- Zurich American Insurance Co. v. Sony Corp. of America et al.

FILED: NEW YORK COUNTY CLERK 05/03/2014 INDEX NO. 651982/2011  
 NYSDJP DOC. NO. 524

1  
 2 SUPREME COURT OF THE STATE OF NEW YORK  
 COUNTY OF NEW YORK: CIVIL TERM PART -  
 3 -----  
 4 ZURICH AMERICAN INSURANCE COMPANY,  
 Plaintiff  
 5  
 6 -against-  
 7 SONY CORPORATION OF AMERICA, SONY COMPUTE  
 LLC, SONY ONLINE ENTERTAINMENT LLC, SONY  
 8 INTERNATIONAL L.L.C, SONY NETWORK ENTERTAIN  
 MITSUI SUMITOMO INSURANCE COMPANY OF AMER  
 9 FIRE INSURANCE COMPANY OF PITTSBURGH, PA.  
 INSURANCE COMPANY, KI INSURANCE COMPANY L.....  
 10 ST. PAUL FIRE AND MARINE INSURANCE COMPANY, GREAT AMERICAN  
 INSURANCE COMPANY OF NEW YORK, A-K INSURANCE COMPANIES  
 11 (FICTITIOUS DEFENDANTS) and 1-2 INSURANCE  
 DEFENDANTS,  
 12 Defendants  
 -----  
 13 40 Centre Street  
 New York, New Yo  
 14 February 21, 2011

BEFORE: HONORABLE: Jeffrey K. Oleg, JSC  
 15  
 16 APPEARANCES:  
 17 Coughlin Duffy, LLP  
 Attorneys for Zurich American Ins  
 18 350 Mount Kemble Avenue, P.O. Box  
 Morristown, New Jersey 07962  
 19 By: Kevin Coughlin, Esq.  
 Robert Kelly, Esq.  
 20  
 21 Nicolaides Fink Thorpe Michaelidis  
 Attorneys for Mitsui Sumitomo  
 22 Insurance Co. of America  
 71 South Wacker, Suite 4400  
 Chicago, IL 60606  
 23 By: Robert S. Marshall, Esq.  
 Amy Klise, Esq.  
 24  
 25  
 26 Delores Hilliard  
 Official Court Reporter  
 - OFFICIAL COURT REPORTER

The question now becomes, was that a publication  
 that was perpetrated by Sony or was that done by the  
 hackers.

There is no way I can find that Sony did that.

In this case my finding is that there was no act or  
 conduct perpetrated by Sony, but it was done by 3rd party  
 hackers illegally breaking into that security system. And  
 that alone does not fall under paragraph E's coverage  
 provision.

# SPECIALIZED “CYBER”/PRIVACY INSURANCE POLICIES

- Privacy And Network Security
  - Provides Coverage for Liability (Defense and Indemnity) Arising Out of Data breaches, Transmission of Malicious Code, Denial of Third-Party Access to the Insured’s Network, and Other Network Security Threats
- Regulatory Liability
  - Provides Coverage for Liability (Defense and Indemnity) Arising Out of Administrative or Regulatory Investigations, Proceedings, Fines and Penalties
- Crisis Management
  - Provides Coverage for Forensics Experts, Notification, Call Centers, ID Theft Monitoring, PR and Other Crisis Management Activities

# SPECIALIZED “CYBER”/PRIVACY INSURANCE POLICIES

- Network Interruption And Extra Expense (and CBI)
  - Provides Coverage for Lost Business Income and Extra Expense Caused By Malicious Code, DDoS Attacks, Unauthorized Access to, or Theft of, Information, and Other Network Security Threats
- Digital Asset Coverage
  - Provides Coverage for Damage To or Theft of the Insured’s Own Systems and Data
- Cyber Extortion
  - Provides Coverage for Losses Resulting From Extortion, e.g., Payment of an Extortionist’s Demand to Prevent a Cybersecurity Incident

# REMEMBERING THE SNOWFLAKE



[back](#)

# Massive Target Hack Traced Back To Phishing Email

Posted: 02/12/2014 3:56 pm EST | Updated: 02/12/2014 5:59 pm EST



2.4k 1188 168 133 232

Like Share Tweet Linked In Email



ADVERTISEMENT



Hackers gained access to Target's computer system and stole financial and personal data of 110 million shoppers by **tricking an employee at an outside vendor into clicking on a malicious email, according to a report** Wednesday by security blogger Brian Krebs.

An employee at Fazio Mechanical, a Sharpsburg, Pa.-based heating, ventilation and air-conditioning company with access to Target's network, fell for a "spear phishing" attack, in which hackers send malware-laced emails that appear to come from trusted sources to take over victims' computers, according to Krebs, who cited sources close to the investigation.

# TRAP EXAMPLE

## I. INSURING AGREEMENTS

### A. DATA BREACH LIABILITY

The Company will pay on behalf of the **Insured** all sums in excess of the Deductible amount stated in the Declarations which the **Insured** shall become legally obligated to pay as **Damages** and **Claims Expenses** resulting from **Claims** first made against the **Insured** and reported to the Company in accordance with the Notice provisions in Section VI of this policy during the **Policy Period**, or **Extended Reporting Period**, if applicable, said **Claim** or **Claims** arising as a result of a **Data Breach Wrongful Act** ~~by the Insured~~, provided that:

- (1) Such **Data Breach Wrongful Act** was committed on or after the **Retroactive Date** and before the end of the **Policy Period**; and
- (2) prior to the **Knowledge Date** stated in the Declarations, no **Senior Executive** knew or could have been reasonably expected to know that such **Data Breach Wrongful Act** might give rise to a **Claim**.

“**Data Breach Wrongful Act**” means any actual or alleged act, failure to act, error, omission, misstatement, misleading statement, neglect, or breach of duty that causes:

- a) **Personal Injury** arising out of a **Privacy Breach** or the **Insured’s Media Content**;
- b) **Unauthorized Access** as a result of any unauthorized act caused by an employee of an **Entity Insured**;
- c) the failure to prevent **Unauthorized Access** to **Computer Systems**;
- d) the inability of a third party, who is authorized to do so, to gain access to **Computer Systems**;
- e) the failure to prevent transmission of **Malicious Code**; and



**BUSINESS INSURANCE****Unintended disclosure, paper records loss most common data breaches: Study**

Judy Greenwald

September 18, 2014 - 1:30 pm ET

A study of more than 1,500 data breaches in 2013 and 2014 by a unit of Beazley P.L.C. reveals that the two most common sources of breaches are unintended disclosure and the physical loss of paper records.



# TRAP EXAMPLE

## I. INSURING CLAUSES

### A. CYBER LIABILITY

The Company shall pay **Loss** on behalf of an **Insured** on account of any **Claim** first made against such **Insured** during the **Policy Period** or, if exercised, during the Extended Reporting Period, for **Injury**.

**Injury** means **Disclosure Injury**, **Reputational Injury**, **Content Injury**, **Conduit Injury** or **Impaired Access Injury**.

**Disclosure Injury** means injury sustained or allegedly sustained by a natural person because of the potential or actual unauthorized access to such natural person's **Record** by another **Person** when such access:

- A. occurs on or after the **Retroactive Date** and before the end of the **Policy Period**; and
- B. results directly from:
  - 1. a **Cyber-attack** into a **System** owned by an **Insured Organization**; or
  - 2. a natural person who has gained unauthorized access to, or has exceeded authorized access to a **System** or **System Output** owned by:
    - i. an **Insured Organization**; or
    - ii. an organization that is authorized by an **Insured** through a written agreement to process, hold or store **Records** for an **Insured**.

BEWARE  
THE

FINE

PRINT



# Q & A



THANK YOU

# K&L GATES

This presentation is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer.