Has the Fortress Been Hacked By Consumers? Cyber Class Actions Are Gaining Steam

Litigation and Dispute Resolution

Technology, Privacy, and eCommerce

CHEAT SHEET

- ***Standing and deliver.*** So far in post-breach class actions, standing has proved the most significant hurdle to plaintiffs.
- ***Et tu, shareholders?*** Due to the stock plunges that often accompany data breaches, shareholders often litigate, claiming breaches of fiduciary duties and securities fraud.
- ***A target on your back.*** Financial institutions burdened by the increase in administrative costs after a breach have litigated class actions successfully.
- ***A temporary reprieve.*** While courts have largely dismissed standing for class action petitioners, two pending US Supreme Court cases may change all that.

If anyone believed that 2014 was the year of the data breach, 2015 was a rude awakening. The Anthem breach alone, discovered in January 2015, affected 80 million members of the health insurer. The November breach at toymaker VTech — a Hong Kong-based global provider of electronic learning products — hit 11 million possible victims. Starwood Hotels & Resorts announced in November 2015 that it discovered an eight-month-long hack of its network and customer data. The recently issued fifth annual survey by Advisen provides some interesting statistics for businesses around the world to consider in 2016:

- At least 92 percent of risk managers consider cyber breaches to be a moderate threat.
- 29 percent said cyber breaches pose a serious threat, a 20 percent increase from 2014.
- 57 percent of respondents assess the threat in using cloud-based services in risk management.
- 43 percent believe that their company has exposure due to the “Internet of Things.”*

* A term coined to describe everyday internet-enabled electronics and devices having the ability to send and receive data.

These statistics confirm that companies continue to become more sensitive to the risks of data breaches. In the wake of massive breaches experienced by companies such as Target, Anthem, and Sony Corp., many businesses either have or are considering the purchase of standalone cyber insurance. Companies of all sizes now must consider whether cyber insurance plays a part in their overall risk management program. In most case the answer should clearly be “yes.”

The focus of this article is the legal exposure that companies may face as a result of class actions related to privacy breaches. Considering the potential size of a class in data breach actions, this type of litigation could be considered the Holy Grail of the plaintiff ’s bar. However, until now, most courts have found in favor of defendants on the basis that the purported class does not have standing under Article III of the US Constitution.

Some additional statistics related to class actions for data breaches are interesting. First, the US District Courts for the Northern Districts of Illinois and California remain preferred venues for plaintiffs. “Approximately four percent of publicly reported data breaches led to class action litigation.” The

retail and credit card industry breaches have been the common focus of class litigation even to the exclusion of more sensitive data, such as Social Security numbers. Finally, while there are myriad causes of action asserted by plaintiffs in such litigation, evidence supports the view that the plaintiffs' bar gravitates to negligence and breach of contract as the primary theories of liability.

Standing is the moat around the fortress

Just as attackers must cross the moat to access the castle, the primary hurdle to a data breach class action is Article III standing. To date, most lawsuits by consumers impacted by data breaches have been unsuccessful for this reason. These lawsuits typically fail at the motion to dismiss stage due to the lack of a cognizable injury. Courts routinely dismiss cases because of a lack of standing where claimed damages largely consist of emotional distress, increased risk of identity theft, and the need to purchase credit-monitoring services. Courts find these types of damages too speculative to support claims.

The US Supreme Court made the issue of standing more difficult following its decision in *Clapper v. Amnesty International USA.* In that case, human rights and media outlets challenged the constitutionality of amendments to the Foreign Intelligence Surveillance Act. The plaintiffs asserted that they had standing to challenge the amendments because they feared their communications would be monitored. They also alleged that the amendments to the law forced them to undertake costly and burdensome measures to protect the confidentiality of communications in order to carry out their job responsibilities.

The Supreme Court held that the plaintiffs lacked Article III standing. The Court reasoned that the plaintiffs' theory of future injuries was too speculative. The Court also noted that plaintiffs could not create standing by making expenditures for monitoring based on a possibility of future harm that may or may not occur.

Following *Clapper*, numerous courts have dismissed data breach class actions for lack of standing.

The most recent appellate court to address the standing issue is the US Circuit Court of Appeals for the Seventh Circuit. The plaintiffs filed a putative class action on behalf of themselves and all other customers of American luxury retailer Neiman Marcus, whose card information was potentially compromised. (Hackers had access to 350,000 credit and debit cards in that breach.) As the court noted, "The plaintiffs point[ed] to several kinds of injury they have suffered: 1) lost time and money resolving the fraudulent charges, 2) lost time and money protecting themselves against future identity theft, 3) the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity, and 4) lost control over the value of their personal information." Not surprisingly, Neiman Marcus raised the drawbridge and successfully moved to dismiss for lack of standing.

On appeal, the Seventh Circuit first considered the injury-in-fact requirement — starting with the *Clapper* factors. The court noted that any alleged "future harm" must be "certainly impending" and that "allegations of possible future injury are not sufficient." The Seventh Circuit held that "*Clapper* does not . . . foreclose any use whatsoever of future injuries to support Article III standing." In finding that plaintiffs whose credit card information was stolen due to the data breach had standing to sue under Article III, the court distinguished the facts of the data breach class action from those in *Clapper*. The court explained that the plaintiffs had shown a substantial risk of harm from the data breach because there was no dispute that various customers' card information had been stolen. The court also noted that "the purpose of [a] hack is, sooner or later, to make fraudulent charges or

assume those customers' identities." Indeed, nearly 10,000 Neiman Marcus customers already had suffered fraudulent charges, which demonstrated actual harm was occurring to customers.

The Seventh Circuit denied Neiman Marcus' petition for rehearing *en banc*. In denying the retailer's petition, the Seventh Circuit confirmed the circuit split on the issue of standing in data breach class actions survives *Clapper*. In 2012, the Supreme Court denied a petition for writ of certiorari to address the question of standing in data breach cases.

More interestingly, the court said that the retailer's offer of free credit monitoring services tacitly acknowledged the likelihood of future unauthorized charges. Offers of credit monitoring are a natural response by most companies in order to maintain customer confidence. In fact, most data privacy insurance policies offer such monitoring within coverage. Now, such a prophylactic measure may prove to be a negative inference in subsequent litigation.

Following the Neiman Marcus ruling, Illinois is emerging as a favored jurisdiction for plaintiffs. However, there may still be defenses available to Neiman Marcus in its case, as the Seventh Circuit returned the matter back to the trial court to consider the retailer's pending motion to dismiss for failure to state a claim.

Given the scope of victims affected by a data security breach and the potentially gargantuan recoveries, litigants have developed creative theories to attempt to overcome the standing hurdle and pursue claims on a class-wide basis. These claims have taken the following forms:

Consumer class actions, brought by those whose personal information was compromised;

Shareholder class actions and derivative suits related to drops in stock price and/or breaches of fiduciary duty; and

Financial institution class actions, brought by entities that incurred administrative costs and increased security as a result of a data breach.

Consumer class actions are the frontal assault on the corporate fortress

The most prevalent type of class action arising from a data breach is from customers whose personal information may have been compromised. It is now expected that a consumer class action will follow any major data breach. Such lawsuits may include claims of negligence, breach of warranty, invasion of privacy, unfair competition, unjust enrichment, violation of state data notification laws, violation of the Computer Fraud and Abuse Act, violation of the Electronic Communications Privacy Act, and violation of the Video Privacy Protection Act. In light of VTech, the Children's Online Privacy Protection Act also may come into play.

For example, in *Sony Gaming Networks & Customer Data Sec. Breach Litig.*, the plaintiffs sued Sony following a breach of its computer systems, resulting in the theft of personal information from millions of Playstation customers. The plaintiffs pursued the following claims against the game maker: negligence; negligent misrepresentation; breach of express warranty; breach of implied warranty; unjust enrichment; violation of state consumer protection statutes; violation of the California Database Breach Act; violation of the federal Fair Credit Reporting Act (FCRA); and breach of the covenant of good faith and fair dealing, which included the fact that wrongful dissemination of sensitive personal

information increased the risk of future harm, regardless of whether actual harm had yet occurred.

The US District Court for the Southern District of California held that the plaintiffs had Article III standing because they plausibly alleged a “credible threat” of impending harm due to the hacking of their personal information. The *Sony* decision has made California another favorite venue for plaintiffs.

In another California case, a federal court held that the plaintiffs had standing to sue Adobe Systems Inc. based on an increased risk of future harm and the cost to mitigate the risk, despite failure to show actual improper use of the stolen information. Relying on *Clapper*, Adobe moved to dismiss all claims arising from a breach of personal information, based on plaintiffs lacked standing to sue.

The district court acknowledged that under the Ninth Circuit’s holding in *Krottner v. Starbucks Corp*., “[T]he possibility of future injury may be sufficient to confer standing” where the plaintiff is “immediately in danger of sustaining some direct injury as the result of the challenged conduct.” The district court declined to rule that Krottner was overruled, and distinguished Clapper based on the likely and high risk that the customers’ personal information would be misused. Common sense would seem to dictate that this information is not being stolen for altruistic reasons.

Shareholder actions and derivative suits as another tactic

Shareholder class actions and derivative suits that allege securities fraud or breaches of fiduciary duties are another type of litigation that can be asserted following a data breach. Securities fraud cases arise when a data breach is closely followed by a marked drop in the company’s stock price.

Heartland Payment Systems was sued by a shareholder purporting to represent a class of shareholders after a stock price drop of nearly 80 percent.

Heartland was the victim of a network breach in late 2007. The company believed that the intrusion had been contained without any sensitive data being acquired by the hackers. The breach was not disclosed. In early 2009, Heartland learned that the earlier attack actually resulted in the theft of 130 million credit and debit card numbers. In subsequent litigation the victims asserted that Heartland management’s statements made during investor conference calls following the 2007 incident regarding its commitment to and adequacy of its data security, as well as its SEC 10-K filing that same year, were materially fraudulent.

The district court dismissed the complaint. The court held that under federal securities fraud laws the mere fact of the security breach did not demonstrate the company had failed to place appropriate emphasis on maintaining a high level of security. The court also held that the plaintiffs did not allege that Heartland knew, or had reason to suspect in 2008, that its security systems were so deficient that it was false or misleading to represent that the company placed significant emphasis on maintaining a high level of security. Because Heartland made a prompt announcement when it discovered card numbers had been stolen, it was not liable to shareholders.

Shareholders may instead decide to pursue a derivative action for breach of fiduciary duty if a securities case is not viable. The decision in *Palkon v. Holmes* demonstrates that plaintiffs in these cases also face significant barriers to success if the corporate decision-makers are diligent and adhere to their duties.

The *Palkon* case arose from three data breaches at Wyndham Worldwide Corp., a well-known hotel

company, that allegedly resulted in the compromise of more than 600,000 card account numbers. In the derivative lawsuit, the plaintiff alleged that the company and its subsidiaries failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner. The complaint also asserted that the individual defendants had not ensured that the businesses implemented adequate data security policies. It also was alleged that the company's operating system was so outdated that the vendor had stopped providing security updates more than three years prior to the hacking.

The district court dismissed the complaint with prejudice. Prior to filing suit, in order to satisfy a threshold requirement for a derivative action, the plaintiff sent a letter to the Wyndham board demanding the company investigate the breaches and pursue claims against the responsible company personnel. The board unanimously refused the demand. The case was dismissed for failure to plead with exactitude that the refusal of the demand was made in bad faith or based on an unreasonable investigation. The court reasoned that the board's refusal of the demand was within the safe harbor of Delaware's business judgment rule. Of course, with each new case plaintiffs' counsel are informed on how to refine their allegations in future cases.

Financial institution class actions look to be a successful attack

A final category deals with financial institutions that incur substantial increased administrative costs related to their customers' data being breached also pursuing class remedies. In these cases, banks and credit card companies are asserting various claims for negligence, negligence per se, negligent misrepresentation by omission, breach of contract, and unfair or deceptive trade practices against companies that are exposed to a data breach. Examples are found in *TJX Cos. Retail Security Breach Litigation* and *Target Corporation Customer Data Security Breach Litigation*.

In the *TJX* case, a class of financial institutions asserted that TJX Companies, owner of retailers Marshalls and T.J. Maxx, violated certain data security system rules imposed by Visa and MasterCard with respect to storing confidential customer information. Banks alleged that the breach injured them because it forced them to reissue debit and credit cards and to monitor accounts for fraud. TJX successfully argued for dismissal of the breach of contract and negligence claims. However, claims for negligent misrepresentation and violation of the Massachusetts Consumer and Business Protection Act remained in the case. After the court denied class certification and returned the suit to state court, many of the banks and associations settled their claims for an undisclosed amount.

In *Target Corporation Customer Data Security Breach Litigation*, a purported class consisting of banks and credit unions sued Target following a massive data breach that exposed 40 million credit and debit cards. The plaintiffs sought, in part, compensation from Target for breach-related expenses, such as reissuing charge cards and covering the cost of responding to the fraud. Target filed a motion to dismiss the complaint on the basis that, in part, it was not liable to banks and credit unions because merchants do not owe a duty of care to payment card issuers when there is intervening criminal conduct.

The US District Court for the District of Minnesota granted in part Target's motion. The court held that the banks and credit unions adequately pleaded general negligence that demonstrated they were foreseeable victims. It is clear from the *Target* decision that the prosecution and defense of data breach claims in financial institution lawsuits will rely in large part on state laws.

Global checklist for purchasing data privacy insurance

- Use a team approach: insured, broker, coverage counsel
- Understand your risk profile
- Review existing coverages to know what coverage is already available
- Put into place other coverage as needed
- Understand that data coverage is broader than just “cyber”
- Ensure there is coverage for using the “cloud”
- Negotiate for a retro date of at least one year
- Know what counsel and vendors will be supplied
- Carefully review the application

What to expect in 2016 and beyond

Businesses can expect consumers and their attorneys to continue seeking class status in light of *Neiman Marcus* and other victories. It also is likely that the issue of standing will make its way back up to the US Supreme Court, due to the split in authority by the appellate courts.

While consumers continue to seek ways to attack the standing fortress, other types of claimants are over the wall at this point. Vendors and businesses are in a better position to assert damages related to breaches. The Target litigation saw class status granted to issuing banks claiming damages from the 2013 breach at the retailer. The court distinguished the banks’ injuries as expenses already incurred for costs by the breach. The court also noted that the financial institutions were not individuals like shopping customers.

While the ruling does not help customers, retailers can certainly expect to see litigation from vendors and other businesses that can piggyback on this ruling.

Consumer settlements have been a rarity because of the success of breached companies in preventing class claims. Of course, a win in court does not necessarily mean a win in the court of public opinion. While customers have had little success in breaching the fortress walls, other victims have fared better.

In addition to credit card issuers, another notable example was Sony employees who were victims of the movie studio’s breach. The breach was traced by the US government to North Korea as retaliation for release of the movie, *The Interview*. Sony settled the employees’ claims, but it remains to be seen whether other companies will do so.

There are two cases currently pending before the Supreme Court that may have an impact on data breach class actions.

The first is *Spokeo, Inc. v. Robins*. *Spokeo* presents the issue of whether Congress can enact a statute that confers Article III standing to sue for statutory damages when the plaintiff has not suffered any actual injury. If the Court addresses this broad issue in its decision, *Spokeo* could have a significant impact on privacy litigation, where plaintiffs often raise novel theories of liability based on alleged technical statutory violations as a means to overcome the common problem of not being able to show a present injury. However, the Court’s analysis is likely to be more narrowly tailored to the

plain language and congressional intent behind the Fair Credit Reporting Act, the particular statute at issue in the case.

The second case is *Tyson Foods, Inc. v. Bouaphakeo*, where the questions presented include the extent to which individual differences in the harm suffered by class members can be ignored and to what extent statistical methods can be used to decide whether to certify a case as a class action. If the decision does involve an examination of the types of statistical evidence that can justify class certification under Rule 23, a ruling may impact future data breach and privacy cases. Similar to other types of cases, statistical methods have been proposed as a way of resolving the problem of variations of injuries and causation between class members found in data privacy cases.

Finally, the Supreme Court recently decided *Campbell-Ewald Co. v. Gomez*, which presented the question of whether an offer of complete relief to a named plaintiff has the effect of mooting both the individual claims and any proposed class claims brought by that named plaintiff. The circuit courts initially split on this question, but recently came into alignment in concluding that an unaccepted offer of settlement does not moot a named plaintiff 's claims. In January 2016, the Supreme Court ruled on this case and held that a full offer of compensation to a named plaintiff, but unaccepted, does not render the case moot. An adverse ruling could have provided defendants facing class action cases a potent weapon to pick off plaintiffs through small settlements in order to prevent class certification. Interestingly, the high Court left the door open to acts by defendants that are more than mere offers to settlement, such as depositing the actual funds of a settlement offer with the court or an account payable to the plaintiff. It is only a matter of time until this theory is tested.

This year should prove an interesting one to see how the future of data privacy cases play out, and how companies respond to inevitable security breaches and associated claims. One thing is certain for companies focused on maintaining the fortress' defenses: the best defense is an aggressive offense. Companies that handle potential data breaches as an enterprise risk management issue are least likely to suffer breaches and the inevitable litigation to follow.

Further Reading

David Zetoony et al., *2015 Data Breach Litigation Report*, Bryan Cave.

See, e.g., Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011); *Allison v. Aetna, Inc.*, No. CIV.A. 09-2560, 2010 WL 3719243, at *5 (E.D. Pa. Mar. 9, 2010); *Hammond v. The Bank of New York Mellon Corp.*, No. 08 CIV. 6060 RMB RLE, 2010 WL 2643307, at *8-9 (S.D.N.Y. June 25, 2010).

133 S. Ct. 1138 (2013).

See, e.g., In re: SuperValu, Inc., 2016 WL 81792 (D. Minn. Jan. 7, 2016); *Green v. Ebay, Inc.*, 2015 WL 2066531 (E.D. La. May 4, 2015); *Remijas v. Neiman Marcus Grp., LLC*, No. 14 C 1735, 2014 WL 4627893, at *5 (N.D. Ill. Sept. 16, 2014) *rev'd and remanded*, 794 F.3d 688 (7th Cir. 2015); *In re Sci. Applications Int'l Corp*. *(SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 34 (D.D.C. 2014); *In re Barnes & Noble Pin Pad Litig.*, No. 12-CV-8617, 2013 WL 4759588, at *6 (N.D. Ill. Sept. 3, 2013); *Polanco v. Omnicell, Inc.*, 988 F. Supp. 2d 451, 471 (D.N.J. 2013).

Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688 (7th Cir. July 20, 2015), *reh'g en banc denied*, Sept. 17, 2015.

Id. at 692.

Remijas, 2014 WL 4627893, at *5.

Reilly, 664 F.3d at 42, *cert. denied*, 132 S. Ct. 2395 (2012).

See, e.g., Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 WL 3511500, at *7 (N.D. Ill. July 14, 2014) (finding Article III's standing requirement was met in a putative data breach class action notwithstanding *Clapper*, but granting motion to dismiss due to the plaintiffs failure to allege actual monetary damages).

996 F. Supp. 2d 942 (S.D. Cal. 2014).

In re Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1216 (N.D. Cal. 2014).

628 F.3d 1139, 1142 (9th Cir. 2010).

Heartland Payment Systems, Inc. Sec. Litig., No. CIV. 09-1043, 2009 WL 4798148 (D.N.J. Dec. 7, 2009).

No. 2:14-CV-01234 SRC, 2014 WL 5341880 (D.N.J. Oct. 20, 2014).

527 F. Supp. 2d 209 (D. Mass. Dec. 18, 2007).

66 F. Supp. 3d 1154, 1158 (D. Minn. 2014).

In re Target Corp. Customer Data Sec. Breach Litig., 64 F. Supp. 3d 1304, 1314 (D. Minn. 2014).

In re Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 490 (D. Minn. 2015).

Spokeo, Inc. v. Robins, 135 S. Ct. 1892, 191 L. Ed. 2d 762 (2015).

Tyson Foods, Inc. v. Bouaphakeo, 135 S. Ct. 2806, 192 L. Ed. 2d 846 (2015).

See Federal Rule of Civil Procedure 23.

Campbell-Ewald Co. v. Gomez, 577 US ___, 136 S.Ct. 663 (2016). 27 Id. 577 US at ___, 136 S.Ct. at 672.

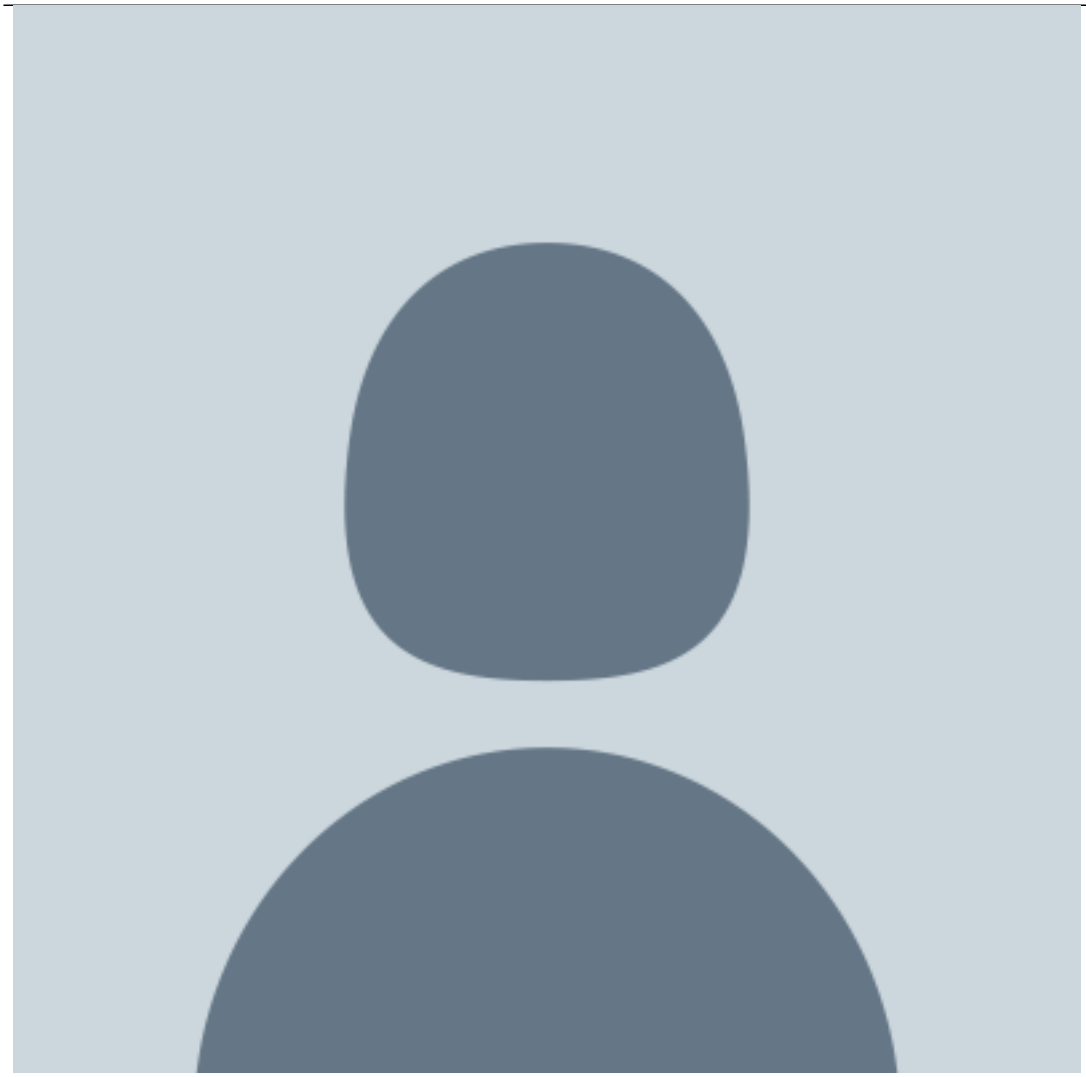
Kimberly R. Hillman

General Counsel

The Winebow Group

She advises the company on numerous corporate and compliance matters, including data privacy and cyber insurance. Hillman received her JD from the University of Baltimore.

Collin J. Hite



Practice Leader of the Insurance Recovery Group

Hirschler Fleischer’s Richmond office

He also is co-chair of the firm’s Data Privacy and Security Group. He handles insurance recovery and coverage litigation nationally, as well as providing insurance policy and program audits for policyholders. Hite received his JD from Southern Methodist University.