Practical Tips for In-House Counsel Anticipating Cyber Class Actions

Daniel B. Garrie, Esq., Co-founder, Law & Forensics; Mediator, Arbitrator, and eDiscovery Special Master, JAMS

Doug Smith, Counsel, Mayer Brown

Mike McGlamry, Shareholder, Pope McGlamry Attorneys At Law



(c) 2022 Lexeprint Inc. All Rights Reserved LLP.

Disclaimer



This is not legal advice, nor should it be considered legal advice.



This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.

Speakers



Daniel B. Garrie, Esq.
Co-founder, Law & Forensics
Mediator, Arbitrator, and
eDiscovery Special Master, JAMS



Doug Smith
Counsel
Mayer Brown



Mike McGlamry
Shareholder
Pope McGlamry
Attorneys At Law

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



This Photo by Unknown Author is licensed under CC BY-SA

Agenda

- Overview
- Data Breach Class Action Settlement Trends
- Practicable Tips for In-House Counsel Anticipating Cyber Class Actions
- Encouragement of Arbitration in Cybersecurity Class Actions
- Impact of Recent Cybersecurity Decisions on In-House Counsel Preparing for Cyber Class Actions
- Questions In-House Counsel Should Consider Regarding Cyber Class Action
- Key Takeaways

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Overview

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Data Breach Class Actions

- Once a security incident occurs, class actions inevitably follow.
- Recent years have shown an increase in the number of cases filed.
- Different settlement templates have been established in these cases.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.


This Photo by Unknown Author is licensed under CC BY-ND

Increase in Data Breach Class Actions

- Almost every industry has been hit by cyber criminals; hotel chains to tech companies to major law firms and even hospitals.
- There will be a surge in data breach class actions as data breaches continue to rise.
- Evidently, cybersecurity is now on the top of the list of major risks companies are facing.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.


This Photo by Unknown Author is licensed under CC BY-SA-NC

Trends in Data Breaches

- In 2021, 43% of data breaches involve small and medium-sized businesses. *Verizon
- The 2022 IBM Cost of a Data Breach Report found that the average total cost of a ransomware breach is $4.62 million, while the average data breach is $4.24 million.
- Moreover, the healthcare industry had the longest data breach lifecycle of 329 days.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



This Photo by Unknown Author is licensed under CC BY-ND

Data Breach Class Action Settlement Trends

- A number of settlements in data breach class actions in federal court this year have provided different settlement trends.
- The biggest settlements in data breach class actions include:
  - Home Depot ($200 Million);
  - Capital One ($190 Million);
  - Uber ($148 Million);
  - Morgan Stanley ($120 Million); and
  - Yahoo! ($85 Million).

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Recent Trends in Securities Class Action

- In 2021, 239 security class action cases were resolved through the dismissal of 153 and 86 through a settlement.
- More than 30% of these cases were filed against companies in the electronic technology and services sector.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



There is an adequately well-established settlement structure.

- Data breach settlements have continued to mainly follow one of two well-established templates.
- This is an injunctive relief and offer of credit monitoring services together with a claims made settlement with a cap or a settlement fund.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Litigation time does not appear to affect the value of the settlement.

- Historically, it has been the understanding of many that aggressive litigation leads to more favorable settlements. However, that is not the case in the data breach realm.
- Despite the amount of time spent litigating, the average per-person all-in settlement amount has been fairly consistent across significant breaches.
- Cases that were determined before any major motions or engagement in discovery were settled for roughly the ‘same per-settlement class member cost as settlements resolved after 2 or 3 years of battle.’ * Morrison Foerster

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Rare Objectors and Appeals

- In the majority of cases, class members do not file objections.
- Roughly 1% of class members object to class-wide settlements. * Vanderbilt Law

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Arbitration Clauses

- Arbitration clauses have become focal points in litigation as companies have decided to include them in contracts to preclude customers' ability to join a class action.
- Forced arbitration clauses are class action bans that prevent consumers from going to court and addressing the full extent of a company's mishaps.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Practicable Tips for In-House Counsel Anticipating Cyber Class Actions

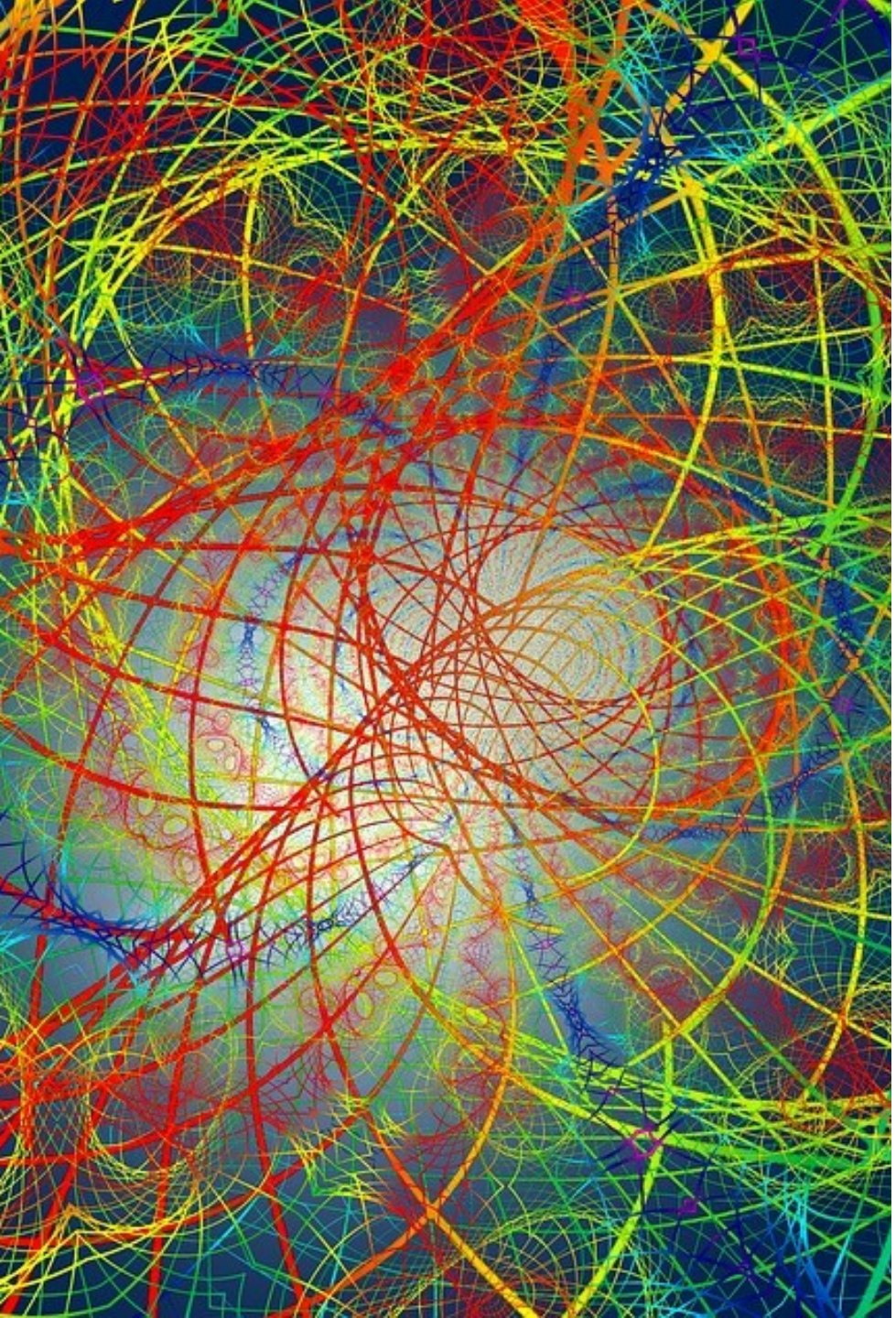
(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Tip 1: Establish a Strong Infrastructure

- In the days or weeks after a company announces a breach, counsel can expect dozens, even hundreds of class actions. These will heavily depend on the nature and scope of the breach.
- In the beginning, companies will rely on counsel to handle dozens or hundreds of lawsuits until the filings slow and navigate the lawsuits into a workable posture.
- Counsel should draft and distribute a legal hold notice. Counsel should also ensure that all auto-delete and similar procedures are disabled while the lawsuits are pending.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Tip 2: Establish Order on the Disarray

- The company will want to consolidate the numerous lawsuits before one court in order to manage the litigation. The company or several plaintiffs' counsel will generally file a petition before the U.S. Judicial Panel on Multidistrict Litigation ("JPML").
- As this process may take some time, local counsel should handle the day-to-day management of these lawsuits. Local counsel will be in the best position to arrange early procedural motions.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Tip 3: Regularly Update Insurers

- Most major companies have cyber insurance that covers data breach litigation.
- These policies usually require the insurer to provide immediate notice and to keep the insurer informed of case developments.
- A dialogue with timely updates should be opened.
- Discussions with insurers are privileged so they will generally be protected from disclosure.





(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Tip 4: Protect the Company from Jockeying by Certain Plaintiffs' Counsel

- It is not rare that some plaintiffs' attorneys will go against the grain to fight for the position as lead counsel.
- They will file ex parte motions regarding document preservation or discovery soon after they file their clients' lawsuits. They will do this to secure a position as lead counsel in the consolidated action because their clients' cases are further along.
- It will be essential for you (in-house counsel) to be prepared to fight these fires, despite the low likelihood of success.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Tip 5: Patience is Key

- The JPML will determine whether cases filed in federal court will be consolidated for pretrial purposes in multidistrict litigation and they only sit every other month.
- 60-120 days can pass before the JPML rule on a request to consolidate lawsuits filed in the backwash of a data breach.
- After this process, it can take 8-10 months or even more between the filing of the initial complaint to the filing of a consolidated complaint in the MDL proceeding.

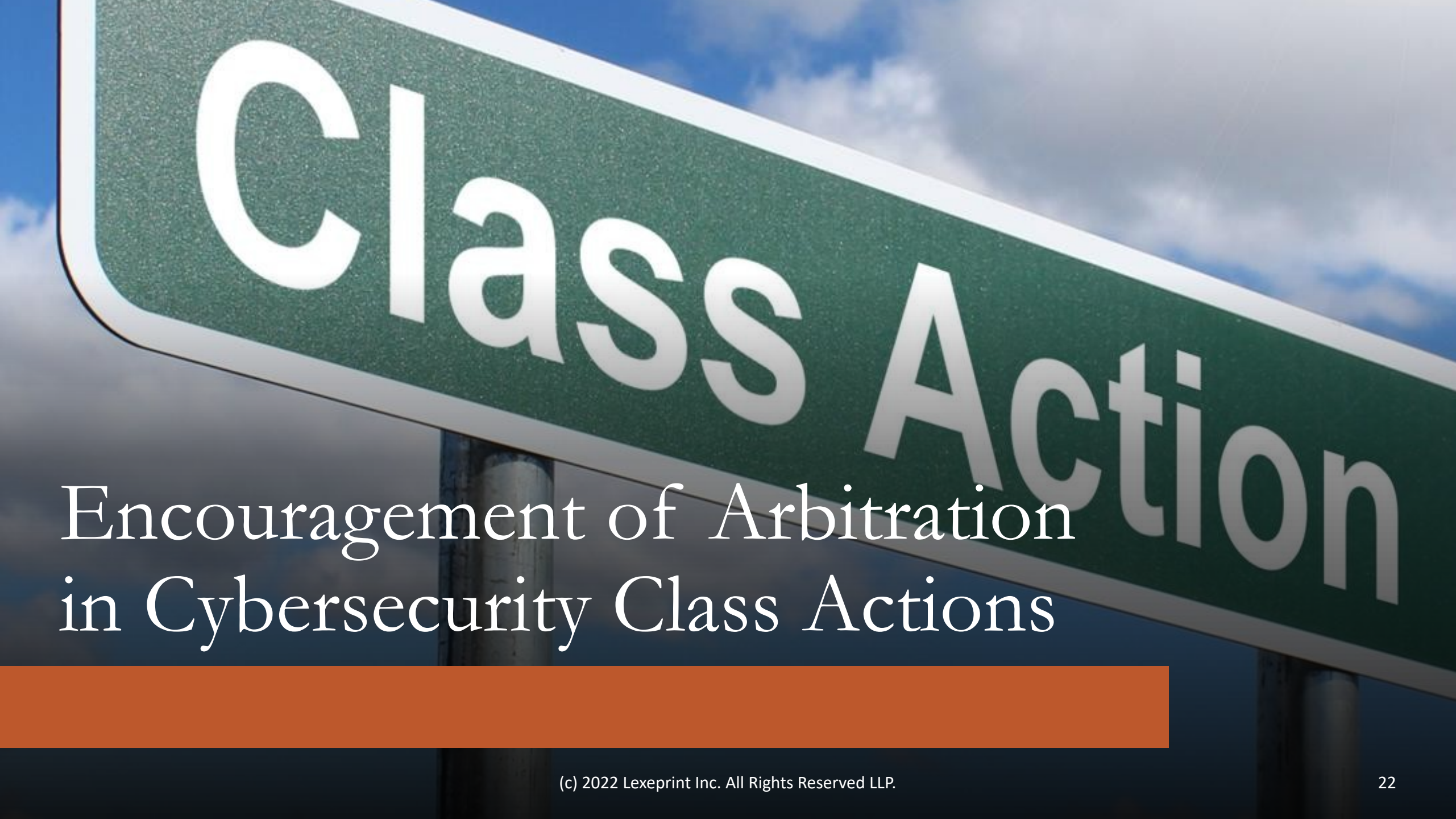
(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Tip 6: Carefully Consider Arbitration Clauses

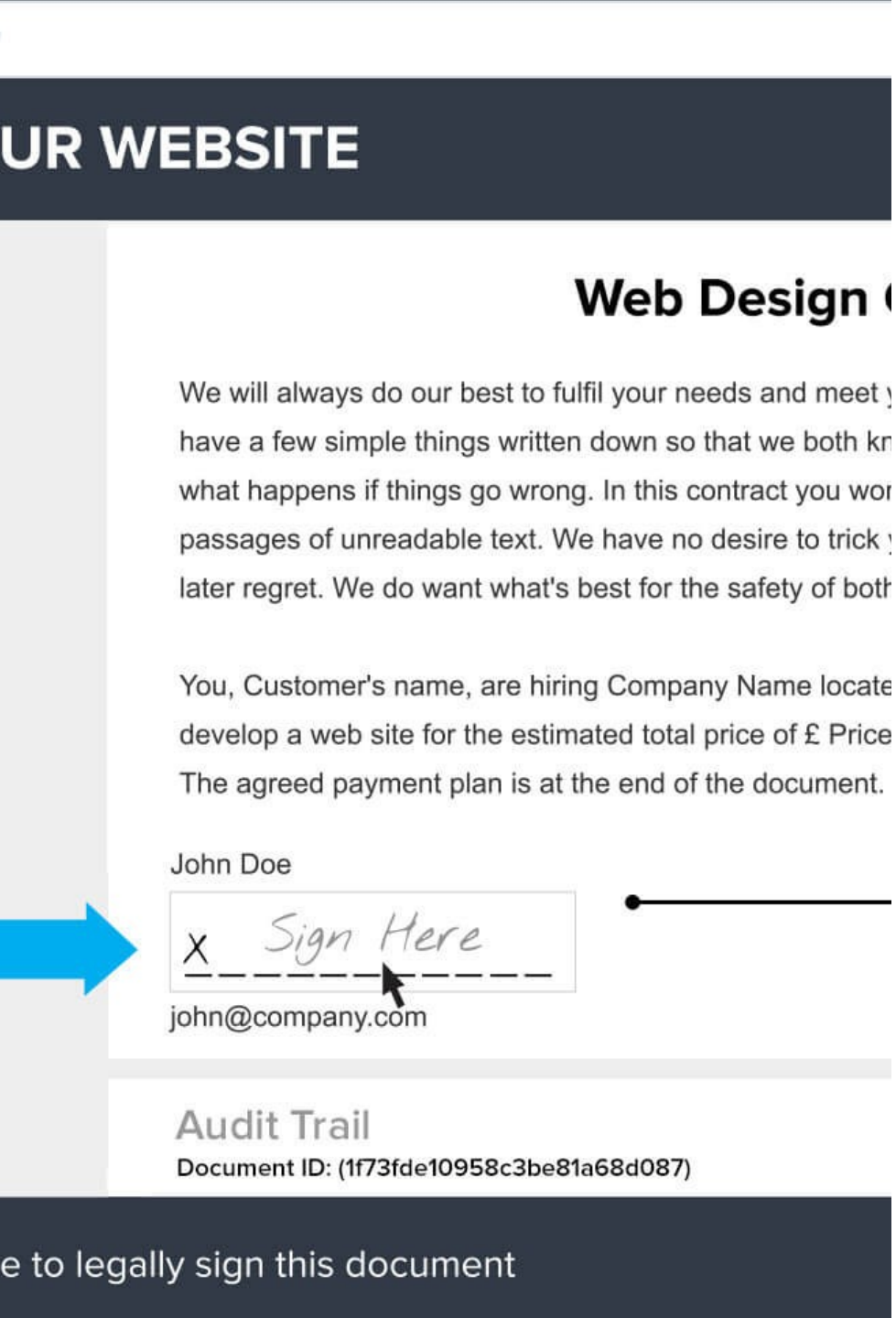
- Private cybersecurity class actions can cost companies enormous litigation fees and potential liability to the proposed class.
- The Supreme Court has noted that individual arbitration involves "lower costs, greater efficiency and speed, and the ability to choose expert adjudicators to resolve specialized disputes."
- Companies should consider adding a mandatory arbitration clause with a class action waiver that is wide enough to include disputes over cybersecurity incidents in their consumers' and employees' agreements.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Encouragement of Arbitration in Cybersecurity Class Actions

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Gutierrez v. FriendFinder Networks, Inc., No. 18-cv-5918-BLF, 2019 WL 1974900 (N.D. Cal. May 3, 2019)

- Facts: The plaintiff was long time user of the adult-oriented dating service Adultfriendfinder.com. He brought a negligence and privacy-related claims against Friendfinder Network (FFN) after they suffered a data breach in 2016. FFN claimed that the plaintiff consented to the terms of the website by making credit card transactions on the site and thus consented to the arbitration clause in the browse wrap agreement once he opened an account and used the site.
- Issue: Did the Plaintiff agree to an arbitration clause within the Terms of the browse wrap agreement?
- Ruling: Gutierrez agreed to the Terms of the website 'despite the absence of evidence that he had ever viewed them.' FriendFinder was granted a motion to compel arbitration.
- Observation: Although the court enforced FriendFinder's terms, the case emphasize the risks associated with using browsewrap agreements.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Yu v. Volt Info. Scis., Inc., No. 19-cv-1981-LB, 2019 WL 3503111 (N.D. Cal. Aug. 1, 2019)

- Facts: The Plaintiff brought a putative class action against his former employer Volt. In August 2018, Volt suffered a data breach. An unknown third party gained access to Volt's computer systems. These systems contained the plaintiff's and other putative class members' 'names, social security numbers, and other personally identifiable information.'
- Issue: Will a court move to dismiss a case and compel a plaintiff to submit his claims to individual arbitration where an arbitration provision is contained in an employment agreement and an employee handbook?
- Ruling: A motion to compel arbitration and conditionally dismiss the case was granted.
- Observations: It is not for the court to determine whether the arbitration provision is unconscionable or whether its scope extends to cover the parties' dispute, it is for the arbitrator.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Vash v. T-Mobile US Inc., No. 1:21-cv-03384, 2021 (N.D. Ga., Aug. 19, 2021)

- Facts: Plaintiff Stephen J. Vash filed a suit seeking compensation for a T-Mobile data breach that compromised the personal data of more than 50 million people. T-Mobile includes a clause to arbitrate disputes as part of the terms and conditions in the agreements when opening an account.
- Issue: Should the court support T-Mobile's forced arbitration clause?
- Ruling: The Court ruled a settlement would be appropriate in this case, which resulted in a$350 million payout that will fund claims by class members, plaintiffs' legal fees, and administrative costs.
- Observation: If the named plaintiffs have opted-out of the arbitration clause, it is possible for a settlement case to proceed.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Impact of Recent Cybersecurity Decisions on In-House Counsel Preparing for Cyber Class Actions

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Re Equifax, Inc. Securities Litigation, 357 F. Supp. 3d 1189, 1218-23 (N.D. Ga. 2019)

- Facts: The plaintiffs alleged that although Equifax made public assurances that it had adequate cybersecurity, its systems had numerous easily-exploitable vulnerabilities that resulted in a cybersecurity incident.
- Issue: Did Equifax take appropriate measures to protect the data of their customers?
- Ruling: The court held that the allegations that Equifax's statements were inaccurate were sufficient to prevent dismissal of the plaintiffs' securities fraud claim.
- Observation: Pre-incident statements about the company's cybersecurity measures can be used to bolster deception-related claims.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



LabMD, Inc. v. F.T.C., 894 F.3d 1221 (11th Cir. 2018)

- Facts: Given the nature of LabMD's work, the lab is subject to data-security regulations. After a billing manager designated the contents of the "My Documents" folder to her computer for sharing, the manager exposed the contents of the files to users outside of the company through the software LimeWire. The FTC investigated the company's data leak and issued an administrative complaint against LabMD.
- Issue: 'Was the FTC's order unenforceable because it did not direct LabMD to cease committing an unfair act or practice within the meaning of Section 5(a)?'
- Ruling: 'Section 5(a), 15 U.S.C.S. § 45(n), of the Federal Trade Commission Act states, as a prerequisite for an act or practice to be unfair, the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.'
- Observations: The FTC's order mandating a complete overhaul of the company's data-security program was unenforceable and vacated.

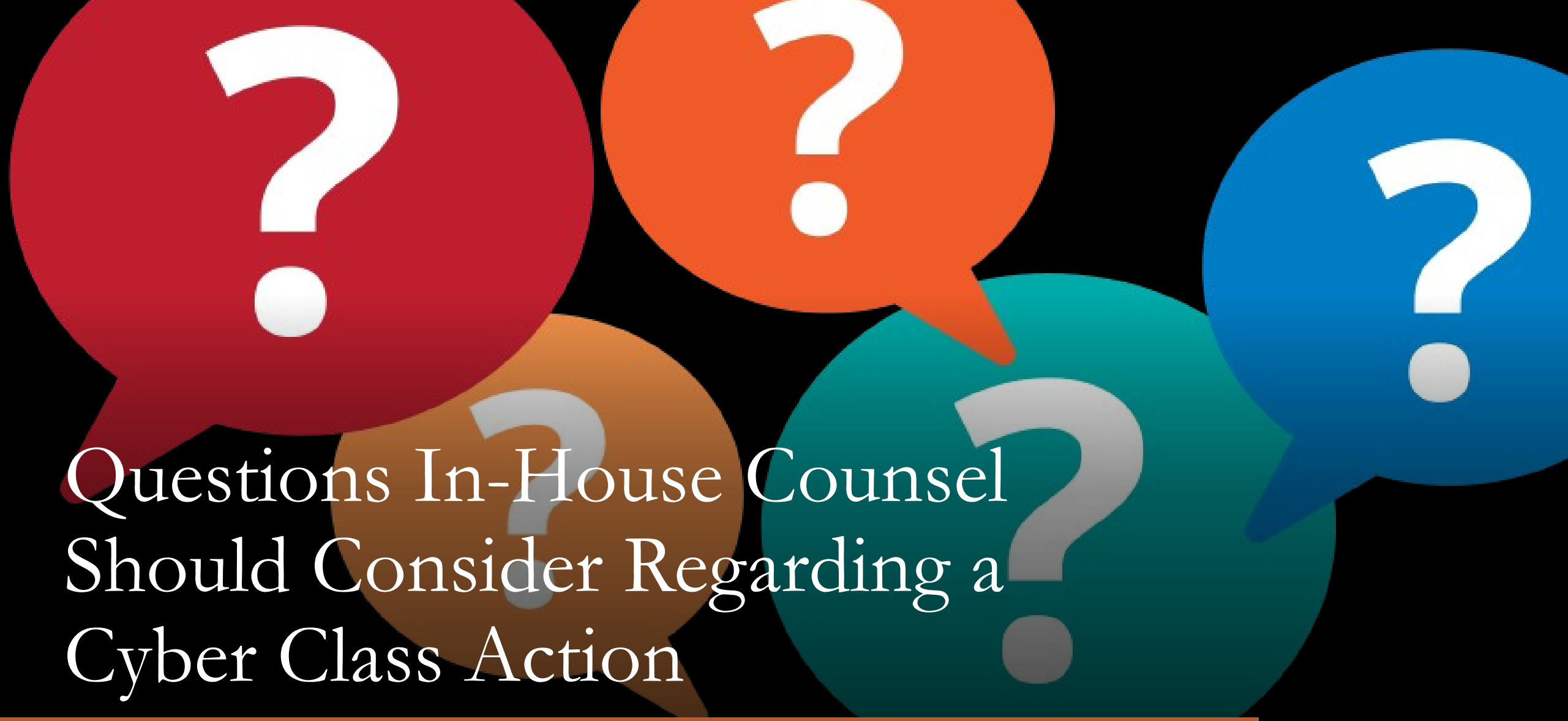
(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Re Zappos.com, Inc., 888 F.3d 1020, 1027 (9th Cir. 2018)

- Facts: In January 2012, hackers breached the servers of Zappos and gained access to the names, account numbers, passwords, email addresses, billing and shipping addresses, telephone numbers, and credit and debit card information of over 24 million consumers.
- Issue: Regardless of the fact that the plaintiffs failed to allege that the hackers used their information in any financial transactions, did the plaintiffs have Article III standing to institute the complaint?
- Ruling: The plaintiffs had Article III standing. "A plaintiff threatened with future injury has standing to sue if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur."
- Observations: A plaintiff must show three things to have U.S. Const. Art II standing. A plaintiff must indicate: "(1) it has suffered an injury in fact that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision."

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Questions In-House Counsel Should Consider Regarding a Cyber Class Action

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.


This Photo by Unknown Author is licensed under CC BY-ND

What actions has the company taken to reduce the likelihood and impact of potential cyber intrusions?

- It is important to have controls that focus on protecting your organization's networks and systems against attacks by external attackers.
- However, as the prevalence of cyber-attacks rise in today's world, it will be equally as important to ensure that your company/organization has a well-developed approach to security once an attacker has entered the network.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



This Photo by Unknown Author is licensed under CC BY-SA

Has the company incorporated and tested an incident response plan?

- While there is no perfect security system, an important means of minimizing the costs of incidents will be through the adequacy of a well-prepared incident response plan.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.


This Photo by Unknown Author is licensed under CC BY-NC-ND

Is the company ready for litigation arising out of a cybersecurity incident?

- It is advisable that in-house counsel and senior leadership at companies understand the nature of cybersecurity claims.
- You should also aim to be able to identify potential resources that can assist you in defending against such claims.
- It may be helpful for companies/organizations to work with their in-house counsel and external counsel to ensure that they can handle the data and privacy practices.
- This will ensure that counsel guiding the company is already well-informed about any key factual aspects of the incident.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



This Photo by Unknown Author is licensed under CC BY-SA-NC

Are there resources in place to help incident response?

- An adequate cybersecurity incident response plan often needs organizations to rely on multiple resources and address the interests of different constituents.
- For example, it may be necessary to engage an external forensic resource and a public communications strategy. It will be most effective to identify potential additional resources before an incident actually occurs.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.


This Photo by Unknown Author is licensed under CC BY

Do the company's insurance policies cover data security incidents?

- It is important that your insurance policies provide your organization with the strongest basis to recover any potentially significant costs and liabilities associated with cyber incidents.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Key Takeaways

- As cybersecurity class action disputes can be a very difficult topic as it crosses multiple legal disciplines and business functions, it will be crucial for in-house counsel and senior leadership at companies to ensure that there is adequate risk mitigation.
- In-house Counsel and senior leadership should aim to accomplish this through adequate planning, business practices and cybersecurity infrastructures in their respect organizations.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



(c) 2022 Lexeprint Inc. All Rights Reserved LLP.

Contact Us



Daniel Garrie
Email: daniel@lawandforensics.com
Phone: 855-529-2466
URL: www.lawandforensics.com



Doug Smith
Email: dougsmith@mayerbrown.com
Phone: (213) 229-5198
URL: https://www.mayerbrown.com



Michael L. McGlamry
Email: mmcglamry@popemcglamry.com
Phone: 404.523.7706 (Atlanta)

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Daniel B. Garrie, Esq.
Law & Forensics LLC – Co-Founder
JAMS – Special Master, Neutral, Arbitrator
Contact:
W: (855) 529-2466
E: daniel@lawandforensics.com
URL: https://www.lawandforensics.com/

LAW & FORENSICS
A Global Legal Engineering Firm

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie, Esq. is the Co-Founder of Law & Forensics LLC, where he heads the Computer Forensics and digital discovery Cybersecurity teams. Daniel has been a dominant voice in the computer forensic and cybersecurity space for the past 20 years, as an attorney and technologist. He is an adjunct professor at Harvard for Computer Forensics and prior to Law & Forensics, he successfully built and sold several technology start-up companies.

Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. He is a mediator, arbitrator, and e-discovery special master for JAMS and is a partner and head of the Cybersecurity at Zeichner, Ellman & Krause LLP. Daniel has both a Bachelor's and a Master's degree in computer science from Brandeis University, as well as a J.D. from Rutgers Law School.

Daniel has led cyber and forensic teams in some of the most visible and sensitive cyber incidents in the United States. He and his team have worked for two of the top five banks in the globe, and dozens of the largest private and public companies in the world. In addition, Daniel has been awarded several patents for advanced cybersecurity and forensic platform he built with his team that is currently used in the industry, TableTop.AI, CustodyTrack.IO, and Forensic Scan.

Daniel is also well-published in the cybersecurity space and has authored more than 200 articles and books. His work is cited by Black's Law Dictionary 10th Ed. In defining the terms "software", "internet", and "algorithm." Lastly, he has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Douglas Smith
Mayer Brown – Counsel
Contact:
E: dougsmith@mayerbrown.com
W: (213) 229-5198
URL: https://www.mayerbrown.com

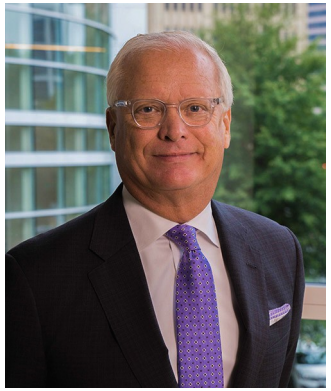
MAYER | BROWN

Doug Smith is counsel in Mayer Brown's Los Angeles office and a member of the Litigation & Dispute Resolution, Cybersecurity & Data Privacy and Supreme Court & Appellate practices. Doug handles complex trial and appellate court litigation, focusing on antitrust, intellectual property, tax-related class actions, and data privacy and cybersecurity.

Before recently joining Mayer Brown, Doug was a litigator with the New York and Los Angeles offices of Skadden, Arps, Slate, Meagher & Flom LLP. He also clerked for The Honorable Beverley B. Martin of the United States Court of Appeals for the Eleventh Circuit, Colorado Supreme Court Justice Richard L. Gabriel while he was on the Colorado Court of Appeals, and Colorado Supreme Court Justice Monica M. Márquez. He also has extensive federal government service, including with the White House's Council of Economic Advisers, the Department of Justice, FDIC, Freddie Mac, the US House of Representatives, and the US Senate.

Doug has a strong commitment to pro bono and has received numerous awards for his pro bono service, including the California Young Lawyers Association's Jack Berman Award of Achievement. Most recently, he argued before the Ninth Circuit and secured his second favorable published opinion on behalf of pro bono clients. He also is a lecturer in law at USC Gould School of Law, teaching a three credit class on Fundamentals of Intellectual Property Law. Doug holds CIPP/US and CIPM certifications from the International Association of Privacy Professionals, He also serves as the Managing Editor of the Journal of Law & Cyber Warfare, and on the board of Neighborhood Legal Services of Los Angeles.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.



Michael L. McGlamry
Pope McGlamry Attorneys At Law – Shareholder
Contact:
E: mmcglamry@popemcglamry.com
W: 404.523.7706 (Atlanta)
URL: https://www.pmkm.com/attorney/mike-mcglamry/#biography

Mike is and has been active representing plaintiffs in personal injury, wrongful death, products and pharmaceutical liability, class actions and mass torts actions that have resulted in verdicts or settlements approaching a billion dollars. Many of these cases were the first such cases in the nation and many involved innovative, ground-breaking legal strategies. He and his partners have long been recognized both in Georgia and nationally as a go-to firm that will take on the most challenging cases and opposition.

In the last few years, Mike has focused on mass tort litigation and has served in leadership roles in several national, high profile, injury cases. Mike has served in leadership roles in the following: NFL Players' Concussion Litigation, U.S. District Court, Eastern District of Pennsylvania, MDL No. 2323 (Plaintiffs' Steering Committee, Co-Lead, Discovery Committee and Communications Committee); Wright Medical Technology, Inc. Conserve Hip Implant Products Liability Litigation, U.S. District Court, Northern District of Georgia, MDL No. 2329 (Co-Lead Counsel); Wright Hip System Cases, Superior Court of the State of California, County of Los Angeles, Judicial Council Coordination Proceeding No. 4710 (Co-Lead Counsel); Biomet M2a Magnum Hip Implant Products Liability Litigation, U.S. District Court, Northern District of Indiana, Cause No. 3:12-md-2391 (Plaintiffs' Steering Committee); Stryker Rejuvenate and ABG II Hip Implant Products Liability Litigation, U.S. District Court, Minnesota, MDL No. 13-2441; Stryker Rejuvenate Hip Stem and ABG II Modular Hip Stem Litigation, Superior Court of New Jersey, Law Division, Bergen County, Case Code 296, Master Case No. BER-L-936-13 (Plaintiffs' Leadership); WellNx Marketing and Sales Practices Litigation, U.S. District Court, Eastern Division of Massachusetts, MDL No. 07-md-1861 (Plaintiffs' Steering Committee). Mike lectures frequently at AAJ, GTLA, and the State Bar of Georgia. In addition, Mike serves on several rules related committees of the Georgia Bar.

Mike and his wife Anne, have 3 beautiful and talented daughters, Caroline, Kate, and Elizabeth. Caroline is now an associate attorney in the firm. In his spare time, Mike remains active athletically; serves as an active member of Haygood United Methodist Church; and supports all things Wake Forest.

(c) 2022 Lexeprint Inc. All Rights Reserved LLP.