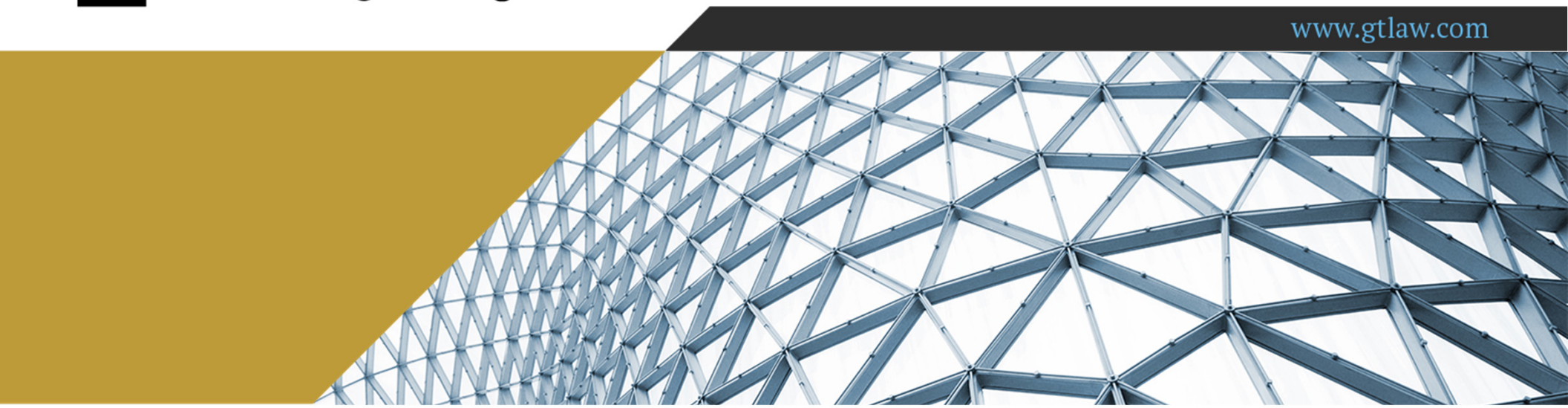
GT GreenbergTraurig

www.gtlaw.com



Strategic Ways to Minimize the Risk of and Prepare for a Data Privacy Lawsuit

NOVEMBER 3, 2022

Rebekah S. Guyon | Rebekah.Guyon@gtlaw.com | 310.586.7716

Today's Presenters

Rebekah Guyon
Shareholder
Greenberg Traurig

Brian Leslie
SVP & General Counsel
Verint

Beth Spain
VP, Associate General Counsel, Litigation and Risk, Signet Jewelers

Seth Presser
Vice President, Legal
Citizen Watch America

New Technologies And Advanced Analytics

- Session Replay Technology Under Increased Scrutiny
  - After-the-fact consent to the recording of online communications rejected by the Ninth Circuit. *Javier v. Assurance IQ, LLC*, 21-16351, 2022 WL 1744107, at *2 (9th Cir. May 31, 2022)
  - Direct-party exception to liability for eavesdropping under Pennsylvania law as applied to a website operator's use of a third-party to record online communications rejected by the Third Circuit. *Popa v. Harriet Carter Gifts, Inc.*, ___ F. 4th _____, 2022 WL 10224949 (3d Cir. 2022)
    - In California, federal courts split on the same issue of website operator liability under California law. *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021); *Graham v. Noom, Inc.*, 533 F. Supp. 3d 823, 832 (N.D. Cal. April 8, 2021)
- California eavesdropping law upheld for non-confidential communications by California Supreme Court
  - *Smith v. LoanMe, Inc.*, 483 P.3d 869, 874 (Cal. 2021)
- New Wave of Video Privacy Protection Act lawsuits arising from websites that do not ostensibly transact in video rental
  - *E.g.*, *Stark et al v. Patreon, Inc.*, No. 3:22-cv-03131 (N.D. Cal. May 27, 2022); *Lamb v. Forbes Media, LLC*, No. 1:22-cv-6319 (S.D.N.Y. July 25, 2022)

Best Practices To Avoid Exposure

- Defenses based in contract
  - Indemnification
  - Who is the data owner?
  - What is the data?
- Consent
  - Who obtains it?
  - How? When?
- Arbitration → Under whose terms?

Data Security and Preventing Data Breaches

- Data security impacts mergers & acquisitions
  - IBM recommends involving cyber risk and cybersecurity leaders early in the M&A lifecycle
  - Data insecurity drives down value
- *Best strategies to mitigate security risk in the realities of a deal lifecycle*

Data Security and Preventing Data Breaches

- *What is a reasonable duty of care for data security?*
  - "Specifically, Plaintiffs contend that Defendants breached this duty by "**stor[ing] customers' information in an unsecure format** (¶ 16), **fail[ing] to require multi-factor authentication** at login (¶ 20), allow[ing] unauthorized users to **link bank accounts to customer accounts without verification** (¶ 15), and **otherwise** implement[ing] **lax security practices** that allowed unauthorized access to Plaintiffs' accounts (¶¶ 17, 46).' . . . . '[t]he consuming public has come to believe that internet companies, which take in their private information, have taken adequate security steps to protect the security of that information from any and all hackers or interventions.'"

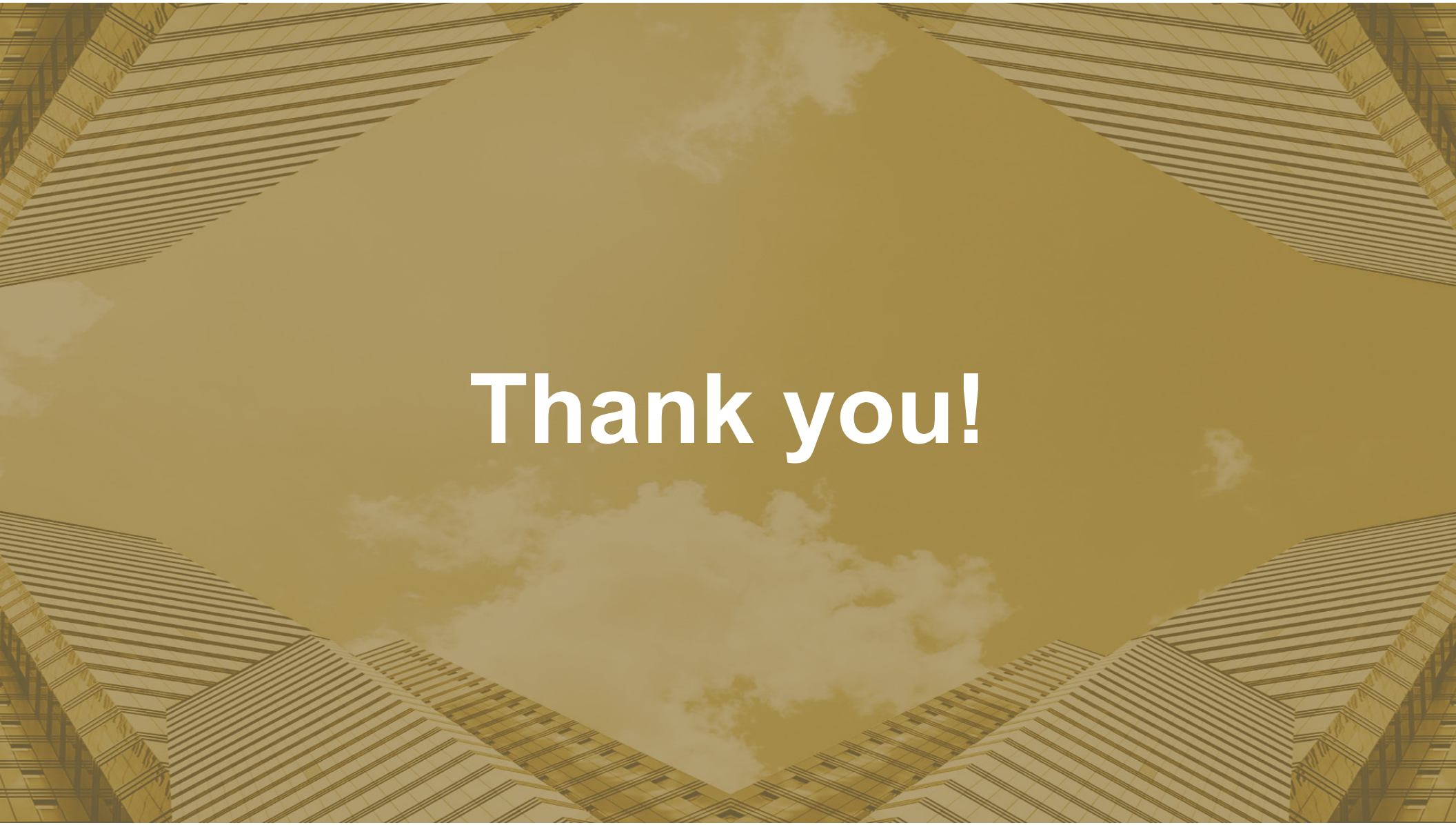
    Mehta v. Robinhood Fin. LLC, 21-CV-01013-SVK, 2021 WL 6882377, at *6 (N.D. Cal. May 6, 2021)
- *When to involve outside counsel in data security assessments?*
  - *Should a cybersecurity firm be on retainer and generate regular written reports?*
    - *In re Capital One Consumer Data Sec. Breach Litig.*, 1:19MD2915 (AJT/JFA), 2020 WL 3470261, at *5 (E.D. Va. June 25, 2020) (report prepared by Mandiant in response to cyber incident held discoverable because it would have been prepared in a similar form pursuant to regular retainer agreement with Mandiant that was not connected to litigation)
    - *Guo Wengui v. Clark Hill, PLC*, 338 F.R.D. 7, 11 (D.D.C. 2021) (outside forensic report held discoverable because defendant did not substantiate "two-track" investigation into security incident with evidence)

Data Security and Preventing Data Breaches

- **Data Minimization**: *In re Drizly, LLC*, FTC File No. 202 3185
  - Mandated Data Minimization Requirements pursuant to proposed Consent Order
  - (1) Drizly required to review the personal information it currently holds and "delete or destroy" anything that is "not being used or retained in connection with providing products or services to [its] customers." Within 60 days, it must also provide a written statement to the commission "specifically enumerating which types of information were deleted or destroyed."
  - (2) Drizly required to establish "data retention limits" through the creation of a retention schedule for personal information, which the company must post publicly on its website. Drizly's public retention schedule must disclose:
    1. The purpose or purposes for which each type of personal data is collected.
    2. The specific business needs for retaining each type of personal data.
    3. A set timeframe for deletion of each type of personal data that precludes indefinite retention of any personal data.

Data Security and Preventing Data Breaches

- **Executive/Officer Responsibility For Data Breaches**
  - *In re Drizly, LLC*, FTC File No. 202 3185 (Oct. 24, 2022): Proposed order includes mandated Information Security Program that follows CEO even after departure from Drizly, LLC
  - *USA v. Sullivan*, Case No. 3:20-cr-00337 (Oct. 5, 2022): Jury finds former Chief Security Officer guilty of obstruction of justice and misprision of a felony in connection with the alleged mishandling of a corporate ransomware attack


Thank you!