SQUIRE PATTON BOGGS

Litigation and Enforcement Round Up For The Advertising Industry

ANA Advertising Law 1-Day Conference

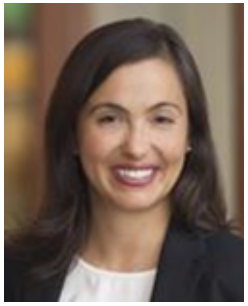
New York City

June 26, 2024

Speakers

SQUIRE PATTON BOGGS

Kristin Bryan
Partner
Squire Patton Boggs
Cleveland/New York



Marisol Mork
Partner
Squire Patton Boggs
Los Angeles

Kyle Dull
Senior Associate
Squire Patton Boggs
Miami/New York

Ericka Johnson
Global Cybersecurity Counsel
TikTok
Washington, D.C.

Agenda

SQUIRE PATTON BOGGS

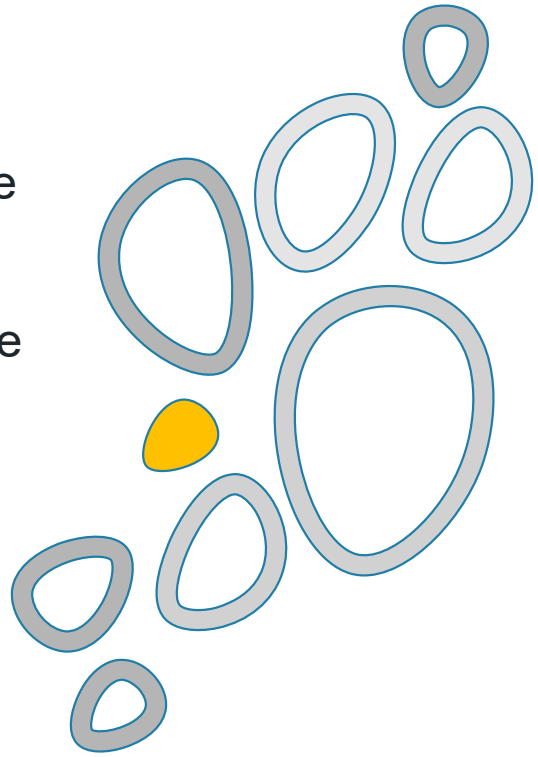
Part 1: FTC Consumer Protection and Data Protection

Part 2: Consumer Protection Enforcement and Guidance

Part 3: Consumer Dispute Trends and Arbitration Update

Part 4: Cybersecurity Developments and Best Practices

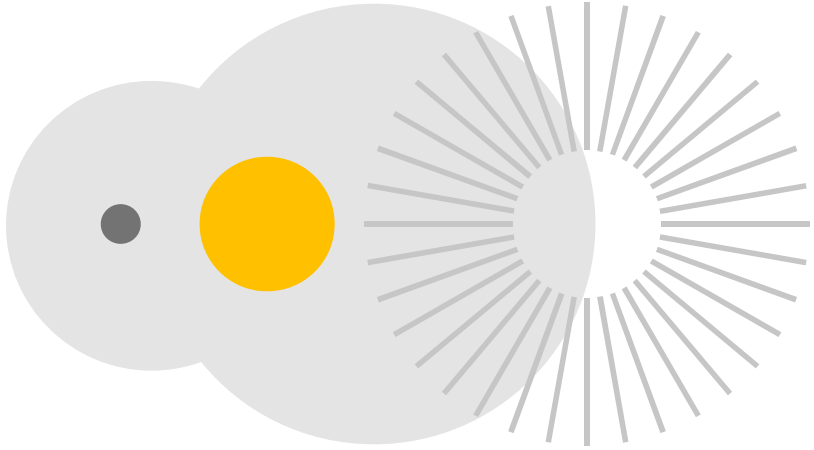
Part 5: Closing



SQUIRE PATTON BOGGS

FTC Consumer Protection and Data Protection

Kyle Dull, Senior Associate, Squire Patton Boggs, Miami/New York



FTC Consumer Protection and Data Protection Insights for 2024

SQUIRE PATTON BOGGS

1. **AI** (it can be used to **advance fraud or has discriminatory impact**);
2. **Dark patterns** to drive sales and frustrate consumer choice (e.g., terminations, opt-outs, etc.), particularly where **driven by tracking and profiling data**;
3. Expect more rulemaking, including advancement of **rulemaking on surveillance capitalism** and likely new rulemaking on data security standards for general commercial enterprises;
4. More than just **deception**. Disclosures of practices may be **insufficient if it is otherwise unfair**, and unfairness authority will be a tool the FTC will not hesitate to use. Areas of potential concerns, where the harm may outweigh benefits to consumers or competition (the Section 5 unfairness standard), include **health-related**, **location** and other **sensitive personal data collection and use**, **engagements with teenagers**, **junk fees** and **business models and algorithms designed to keep a consumer overly engaged**.
5. So-called "**negative option**" subscriptions services will be a focus (though no timeline was given for completion of rulemaking), as will be door-to-door sales, robocalls and privacy practices, including but not limited to practices of data brokers.
6. As the **Green Guides** rulemaking is advanced, the FTC will be working to develop standards that are consistent with **environmental claims** rules in Europe and other advanced economies.

Mid 2023: Target on Health and Health-ish Data

SQUIRE PATTON BOGGS

- The FTC issued three high-profile orders (GoodRx, BetterHelp, and Premom) involving alleged violations of **deceptive and unfair activities** under Section 5 of the FTC Act and, in some cases, violation of HBNR.
- These orders, while they are merely settlements of claims brought under a number of theories, including allegations of deception, and are not rulemakings, **suggest that the FTC expects businesses to obtain consent for the use of consumer health information for ancillary purposes**, such as targeted advertising, and otherwise clarifies when a digital health application needs consent to share data.
- The unfairness claims, and the treatment of consumer health information as highly sensitive, lay the foundation for a **consent-based standard** even without specific federal statutory or regulatory obligations, such as is the case when the HBNR applies (e.g., mobile apps collecting consumer health information from multiple sources).

Sensitive Data Processing is in the FTC's Crosshairs

SQUIRE PATTON BOGGS

Kochava, In-Market, and X-Mode/Outlogic

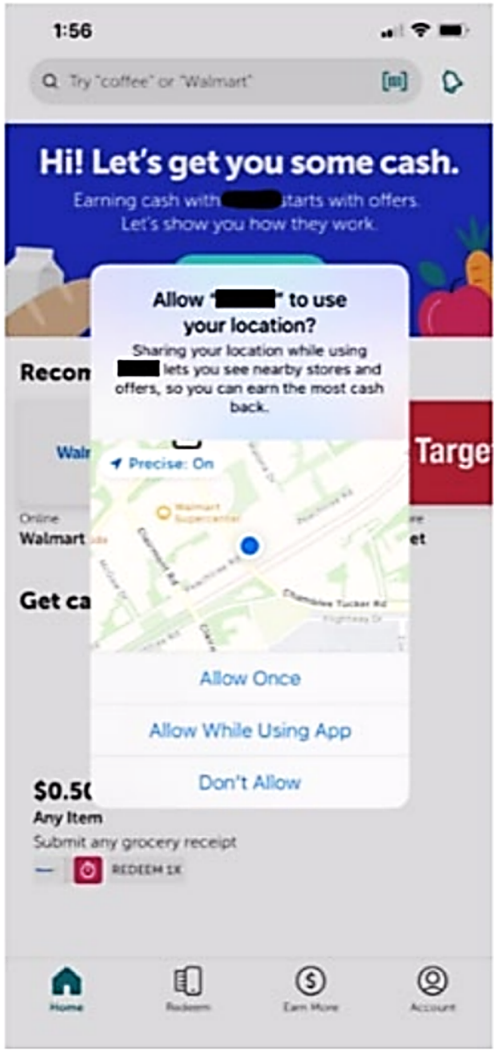
- Consumer tracking has been of interest to the FTC for some time now and the FTC has attempted to address the topic in different ways, including supporting proposed federal Do Not Track legislation, through its power to prohibit deception, and most recently unfairness claims.

Remember the FTC's Vizio settlement?

- Collecting and sharing such data, without the consumer's consent, was deemed to have caused substantial injury to the consumers, and this injury was sufficient to warrant a finding of unfairness, at least according to the FTC.

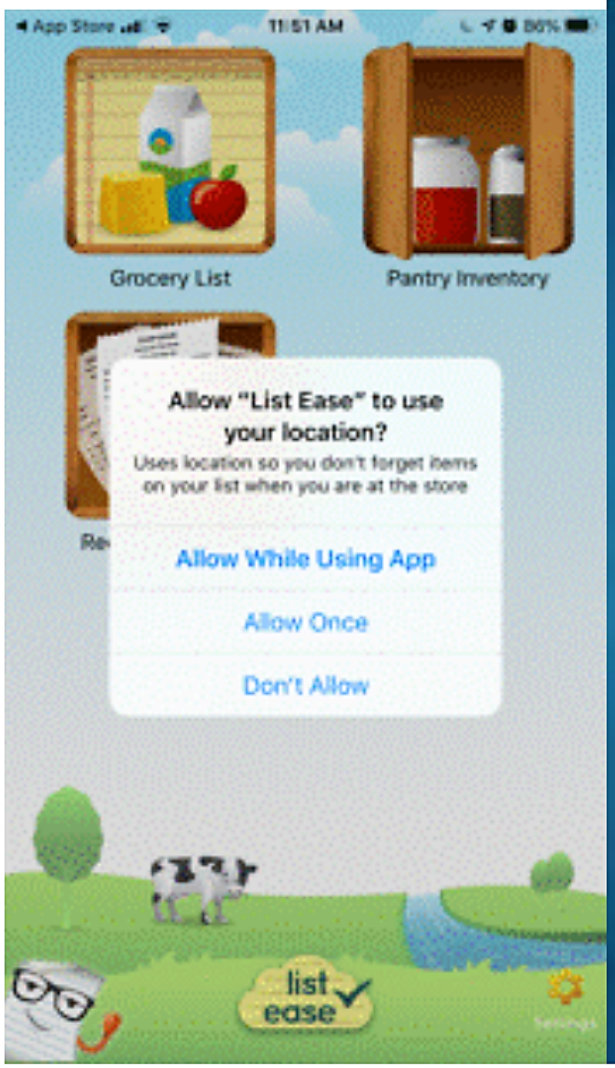
SQUIRE PATTON BOGGS

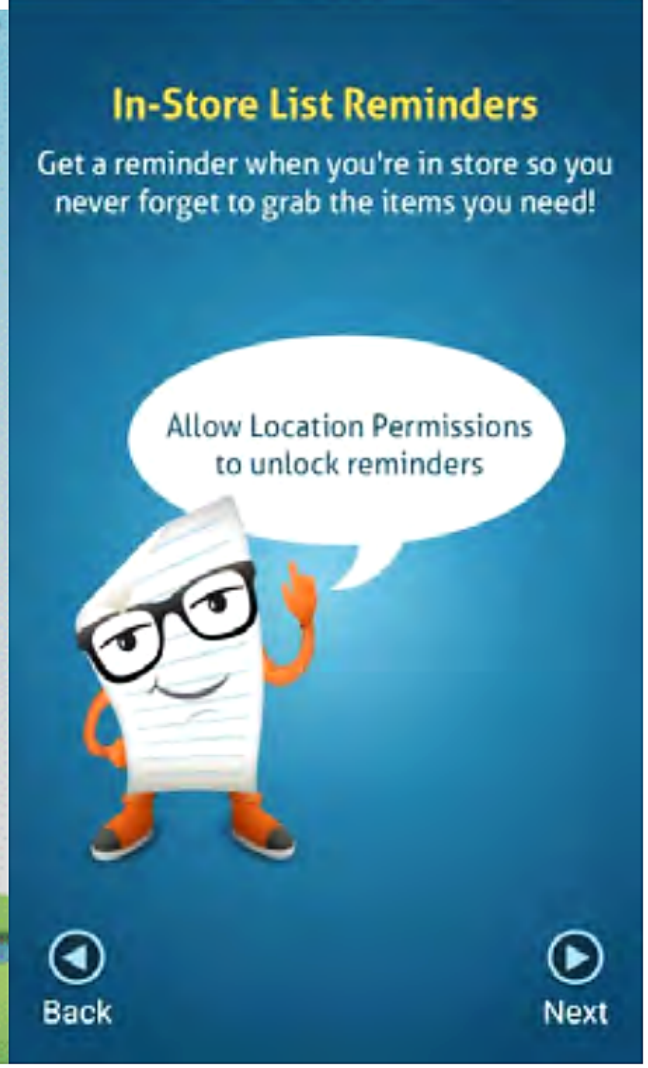
Kochava



SQUIRE PATTON BOGGS

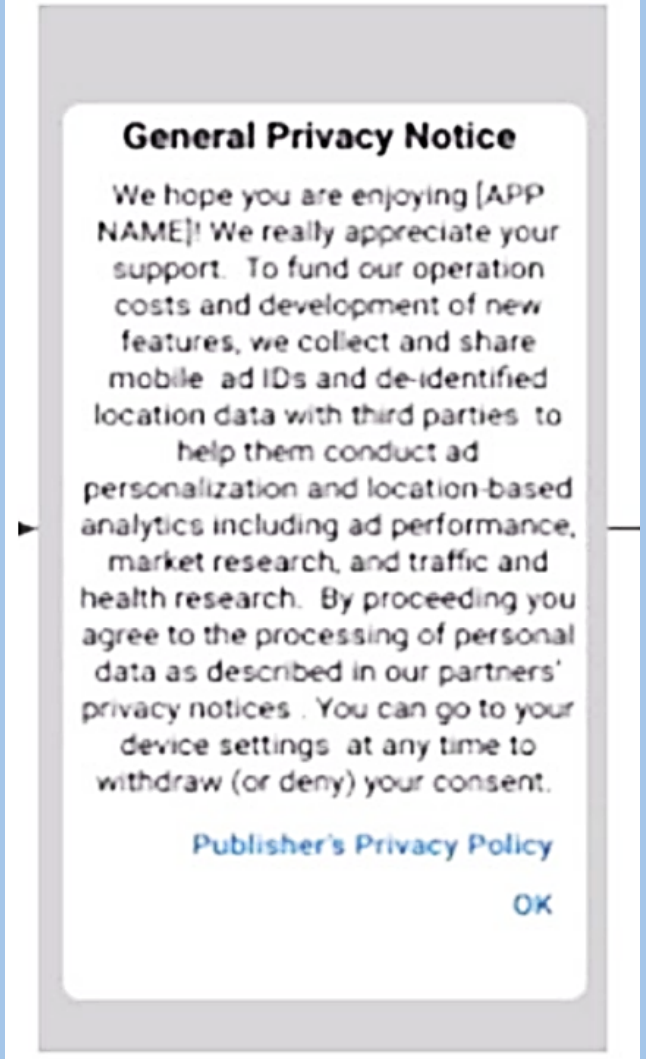
InMarket Media





SQUIRE PATTON BOGGS

X-Mode



Kochava, In-Market, and X-Mode/Outlogic Takeaways

SQUIRE PATTON BOGGS

- Geolocation data paired with a persistent identifier, such as an advertising or device ID, even if not directly connected to a named individual consumer, is sensitive personal data according to the FTC.
- Before a business can collect, sell, or share sensitive personal data (*or at least precise location*) the business must either:
  - Effectively provide the consumer with sufficient disclosures describing the categories of information collected, the purpose, the types of entities receiving the data, and a simple mechanism for consumers to opt-out or withdraw consent; or
  - Obtain the consumer's express, affirmative consent to the collection, sale, or sharing of sensitive personal information.
  - In either case, the FTC will apply its clear, conspicuous and proximate standards to the notices.

Kochava, In-Market, and X-Mode/Outlogic Takeaways

SQUIRE PATTON BOGGS

- Substantial injury ("likely to cause substantial injury") to consumers, a requirement to establish unfairness under Section 5, can be established by the mere risk that location data could be used to identify people and track them to sensitive locations (e.g., medical facilities, LGBTQ+ associated locations, etc.), because that may expose consumers to secondary harms (e.g., stigma, discrimination, physical violence, emotional distress, etc.) or it may be an invasion of the consumer's privacy.
- Businesses that use, or allow others to use, tracking technologies to track consumers should consider providing consumers with enhanced disclosures regarding the use of such tracking technologies and how opt-out of the tracking, especially if sensitive information is involved.

Health Breach Notification Rule

SQUIRE PATTON BOGGS

(Amendments effective July 29, 2024)

- Revising and adding **definitions** to clarify how the rule applies to **health apps** and similar technologies, and what it means to draw from multiple sources.
- **Redefine breach of security** to clarify it "includes an unauthorized acquisition of PHR identifiable health information in a personal health record that occurs as result of a data security breach or unauthorized disclosure."
- Clarify that a "**PHR related entity" includes** those "that offer products and services through the online services, including mobile applications, of vendors of personal health records" and only those "entities that access or send unsecured PHR identifiable health information to a personal health record."
- Permit **notice by electronic means** in certain circumstances, **expand the content required** in notices, and **provide exemplar** notices.
- An expansive **definition of "clear and conspicuous**" that, for online disclosures, requires the placement of notices or a link to the notice "on screen[s] that consumers frequently access."

FTC Data Protection Key Takeaways:

SQUIRE PATTON BOGGS

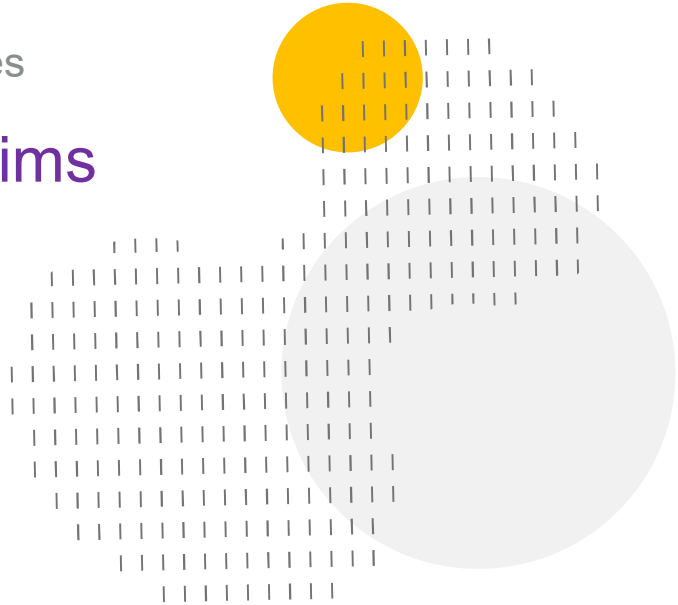
1. The FTC has an aggressive approach to addressing non-HIPPA-regulated health data practices, and an expansive approach as to what is sensitive data.
2. Identify what data is being collected and shared with third parties.
3. Review consumer flow to ensure that sufficient disclosures are being made and proper consents are being collected.
4. Conduct regular audits to ensure that policies and procedures are in place and being followed.
5. Identify outside counsel who can assist you with meeting your obligations.

SQUIRE PATTON BOGGS

Consumer Protection Enforcement and Guidance

Marisol Mork, Partner, Squire Patton Boggs, Los Angeles

Update: Made in USA and Green Claims



Made in USA Labeling Rule

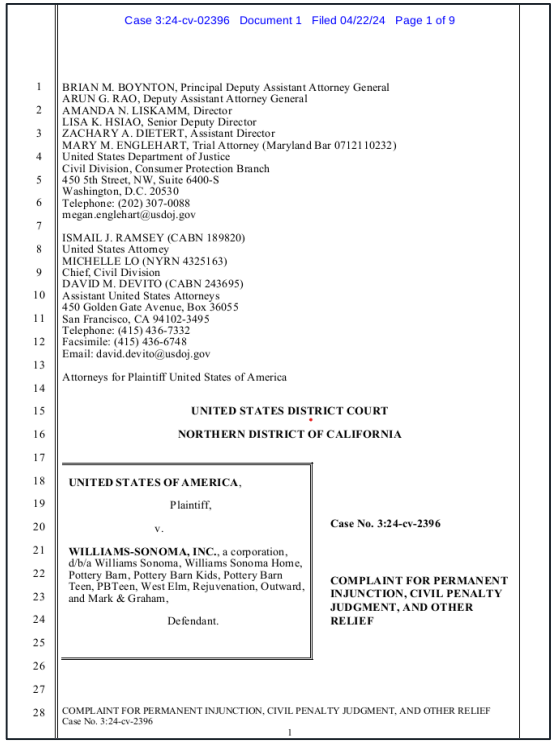
SQUIRE PATTON BOGGS

- Unqualified Made in USA Claim
  - Final assembly or processing of the product occurs in the United States;
  - All significant processing that goes into the product occurs in the United States; and
  - All or virtually all ingredients or components of the product are made and sourced in the United States

Enforcement Actions

- January 25, 2024 Settlement:
  - Kubota North America Corp. required to pay a $2 million civil penalty for falsely labeling replacement parts as MUSA.
  - Unqualified MUSA claims prohibited unless final assembly or processing – and all significant processing – takes place in the U.S. and all components are made and sourced in U.S.
  - Qualified MUSA claims must include a clear and conspicuous disclosure about the extent of foreign content or processing.
  - U.S. assembly claims are only permitted if product is last substantially transformed in the U.S., principal assembly takes place in the U.S. and U.S. assembly operations are substantial.

Enforcement Actions



Case 3:24-cv-02396 Document 1 Filed 04/22/24 Page 1 of 9

BRIAN M. BOYNTON, Principal Deputy Assistant Attorney General
ARUN G. RAO, Deputy Assistant Attorney General
AMANDA N. LISKAMM, Director
LISA K. HSIAO, Senior Deputy Director
ZACHARY A. DIETERT, Assistant Director
MARY M. ENGLEHART, Trial Attorney (Maryland Bar 0712110232)
United States Department of Justice
Civil Division, Consumer Protection Branch
450 5th Street, NW, Suite 6400-S
Washington, D.C. 20530
Telephone: (202) 307-0088
megan.englehart@usdoj.gov

ISMAIL J. RAMSEY (CABN 189820)
United States Attorney
MICHELLE LO (NYRN 4325163)
Chief, Civil Division
DAVID M. DEVITO (CABN 243695)
Assistant United States Attorneys
450 Golden Gate Avenue, Box 36055
San Francisco, CA 94102-3495
Telephone: (415) 436-7332
Facsimile: (415) 436-6748
Email: david.devito@usdoj.gov

Attorneys for Plaintiff United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,

Plaintiff,

v.

WILLIAMS-SONOMA, INC., a corporation, d/b/a Williams Sonoma, Williams Sonoma Home, Pottery Barn, Pottery Barn Kids, Pottery Barn Teen, PBTeen, West Elm, Rejuvenation, Outward, and Mark & Graham,

Defendant.

Case No. 3:24-cv-2396

COMPLAINT FOR PERMANENT INJUNCTION, CIVIL PENALTY JUDGMENT, AND OTHER RELIEF

COMPLAINT FOR PERMANENT INJUNCTION, CIVIL PENALTY JUDGMENT, AND OTHER RELIEF
Case No. 3:24-cv-2396

1

- April 25, 2024 Settlement:
  - Williams-Sonoma required to pay a record civil penalty of $3.175 million for violating a 2020 FTC Order re MUSA claims.
  - Unqualified MUSA claims prohibited unless final assembly or processing – and all significant processing – takes place in the U.S. and all components are made and sourced in U.S.
  - Qualified MUSA claims must include a clear and conspicuous disclosure about the extent of foreign content or processing.
  - U.S. assembly claims are only permitted if product is last substantially transformed in the U.S., principal assembly takes place in the U.S. and U.S. assembly operations are substantial.

Investigations re MUSA Claims

- May 17, 2024 closing letter to ROKA Sports, Inc.:
  - "[M]arketing materials may have overstated the extent to which ROKA eyewear is made in the United States. Specifically, although ROKA broadly advertised its eyewear as 'Handbuilt in USA' or 'Handbuilt in Austin, TX,' certain products incorporated imported glasses frames, lenses, or other significant components."
  - Alternative qualified claims:
    - "Made in USA of Imported Parts"
    - "Made in USA from French and Korean Parts"
    - "60% U.S. Content"
  - FTC decided not to pursue the investigation further based on ROKA's remedial response.

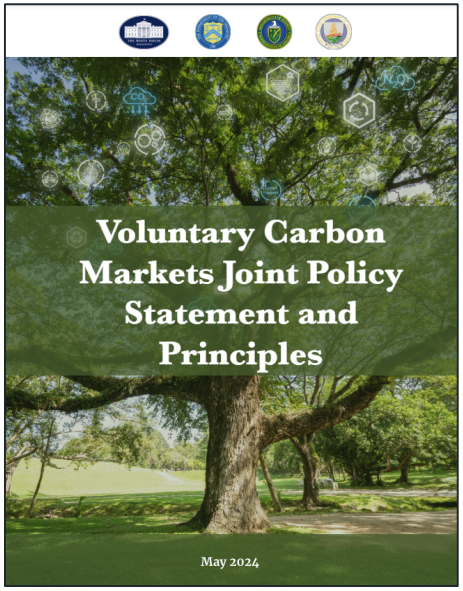
Litigation: “Carbon Neutral” Claims

- Complaint: “Carbon neutral” claim on Evian’s packaging is false and misleading because “reasonable consumers reviewing the Product's label and packaging would believe the manufacturing of the Product is sustainable and does not leave a carbon footprint.”
- Motion to dismiss granted/denied in part: “‘Carbon neutral’ is an ambiguous term, and evidence shows that consumers are confused by it.”
- Takeaways:
  - Heightened litigation risk for carbon neutral claims
  - Proximity of qualifications matter
  - Ensure compliance with Green Guides

CA Climate Disclosure Laws

- Voluntary Carbon Market Disclosure Act
  - Disclosure compliance pushed to January 1, 2025
- Climate Corporate Data Accountability Act
  - (SB-253)
  - Reporting requirements set to take effect in 2026.
- Climate-Related Financial Risk
  - (SB-261)
  - Reporting requirements set to take effect in 2026.

Substantiating Net-Zero – Voluntary Guidelines on Carbon Offsets

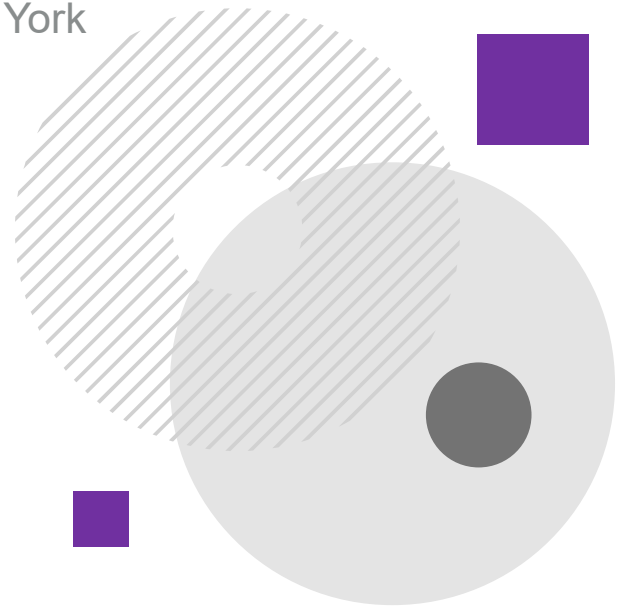


1. Carbon credits and the activities that generate them should meet credible atmospheric integrity standards and represent real decarbonization.
2. Credit-generating activities should avoid environmental and social harm and should, where applicable, support co-benefits and transparent and inclusive benefits-sharing.
3. Corporate buyers that use credits ("credit users") should prioritize measurable emissions reductions within their own value chains.
4. Credit users should publicly disclose the nature of purchased and retired credits.
5. Public claims by credit users should accurately reflect the climate impact of retired credits and should only rely on credits that meet high integrity standards.
6. Market participants should contribute to efforts that improve market integrity.
7. Policymakers and market participants should facilitate efficient market participation and seek to lower transaction costs.

SQUIRE PATTON BOGGS

Consumer Dispute Trends and Arbitration Update

Kristin Bryan, Partner, Squire Patton Boggs, Cleveland/New York



Dispute Update: Focus on California Continues

SQUIRE PATTON BOGGS

- Plaintiff's bar continuing to focus on claims arising under California law, particularly those arising under state's wiretapping law
  - California Invasion of Privacy Act ("CIPA"): Private right of action, $5,000/violation without showing of actual harm required
  - Meta pixel, session replay, chat features
  - Over 500 cases filed in state and federal court in past few years against website operators, majority of these are in California.
  - Core issues in these cases usually revolve around consent to practices at issue, whether information involved can constitute "contents" of communication.

Websites as a Trap and Trace/Plaintiff's Attempt to Criminalize the Internet

SQUIRE PATTON BOGGS

- Federal law prohibits law enforcement's use of pen register or trap and trace devices without a court order
- Many states, including California, have similar statutes
- Application of these laws have been traditionally limited to physical devices that record the numbers dialed from a specific telephone line, or the originating numbers of calls placed to the line
- Plaintiff's bar looking to expand the scope of these laws to apply to the internet
- 150+ cases filed since last year
- on arcane provisions of the California Invasion of Privacy Act (CIPA) that restrict

Arbitration to Mitigate Litigation Risk: Not A Silver Bullet, Even With Class Action Waiver

SQUIRE PATTON BOGGS

- Consumer arbitration provisions with class action waiver increasingly included in online terms, with either AAA or JAMS named to hear disputes.

- Traditional Advantages of Arbitration Include:
  - Less Costly/Time Consuming
  - Private
  - Streamlined discovery and motion practice
  - Result in one case not binding precedent for others

Mass Arbitration: Flip the Script Against Defendants

SQUIRE PATTON BOGGS

- Mass arbitration first emerged with wage and hour and discrimination claims
- Use by plaintiff's bar recently expanded to include privacy claims arising under state law (e.g., CIPA, BIPA)
- Way for plaintiffs to weaponize requirement of individual arbitration of claims
- Online solicitation of hundreds, if not thousands of individual claimants to simultaneously commence arbitration against defendant
- Compels defendant to pay hundreds of thousands or millions in upfront filing fees before even start litigating merits of underlying claims

For instance:

- Uber: Loses appeal to block $92 million in mass arbitration fees.
- Samsung: Ordered to pay over $4 million in mass arbitration initiation fees (appeal pending before Seventh Circuit)

AAA, JAMS Have Both Introduced Mass Arbitration Procedures But Challenges Persist

SQUIRE PATTON BOGGS

- **Positive developments include:**
  - Signed affirmation now required
  - Updated fee schedules
  - Availability of a process administer for certain issues
  - Expanded role of mediation
- **Challenges remaining include:**
  - Limited options for challenging frivolous claims
  - Filing fees still burdensome
  - Process administrator limited in jurisdiction
  - Practice of requesting waiver of certain contractually agreed to protections in arbitration agreement if violates AAA or JAMS procedures (e.g., damages limitations, arbitration location)
- **Mitigation Options**
  - Further revisions to TOS to address mass arbitration
  - Discontinuation of arbitration
  - Others

SQUIRE PATTON BOGGS

Cybersecurity Developments and Best Practices

Ericka Johnson, Global Cybersecurity Counsel, TikTok

Case Study: In the Matter of Blackbaud, Inc.

SQUIRE PATTON BOGGS

- Ransomware attack in 2020.
- Blackbaud paid 24 bitcoin (~$250,000) in ransom in exchange for the threat actor's promise to delete stolen data. Blackbaud could not confirm whether stolen data was deleted.
- Later, multiple consumers submitted complaints alleging attempted identity theft and fraud using personal data affected by the incident.

Litigation and Enforcement Actions

- In the aftermath of the cyberattack, Blackbaud was investigated by multiple government authorities and targeted with private lawsuits.
- Blackbaud settled with state regulators ($49,500,000), the U.S. Federal Trade Commission, and the U.S. Securities Exchange Commission ("SEC") ($3,000,000) in 2023 and 2024, almost four years after it first experienced the cyberattack.

FTC Investigation Findings

SQUIRE PATTON BOGGS

1. Misrepresented data security practices in public-facing privacy policy (i.e., that it used reasonable and appropriate safeguards to protect consumers' personal data) because Blackbaud did not, among other things, implement and enforce
   - employee password controls;
   - multi-factor authentication;
   - log monitoring;
   - appropriate data retention, deletion and encryption policies;
   - firewall controls;
   - and network segmentation.
   - Blackbaud also did not conduct regular tests of its security controls, risk assessments, vulnerability scans, and penetration testing of its networks and databases.
2. Failed to issue timely breach notifications, misrepresented investigation findings (i.e., "[n]o action required on your end because no personal information about your constituents was accessed" when in fact, the opposite was true).
3. Failed to provide update incident notifications as additional material information became available.

FTC Order

SQUIRE PATTON BOGGS

- Mandatory data deletion of customer backup files containing customers' personal data that is not being retained in connection with providing products and services to Blackbaud's existing customers.
- Prepare and implement a publicly available data retention schedule for customer backup files containing customer personal data that includes definite timeframes for deletion (no indefinite retention).

Key Takeaways FTC Enforcement Action

1. If you publicly represent that you use reasonable and appropriate safeguards to protect consumers' personal data, make sure you are implementing and enforcing reasonable and appropriate safeguards across the data life cycle (including for backup data in storage).
2. Update software regularly, including legacy products, if updates become available.
3. Do not store data for longer than necessary and delete former customers' data if possible.
4. Conduct diligent investigation of cyber incidents and ensure incident notifications accurately reflect the factual findings of the investigation.
5. Provide timely incident notifications to affected individuals, regulators, and/or the media, and provide timely updated notices, as appropriate, if ongoing investigation reveals material information requiring updates to prior notice(s).

SEC Investigation and Key Takeaways

SQUIRE PATTON BOGGS

- According to the allegations, in the notices provided to its non-profit customers, Blackbaud indicated, inaccurately, that the threat actor did not access any donor bank account information or SSNs.
- Blackbaud a Form 10-Q discussing the incident, but characterizing access to donor bank account information and SSNs as hypothetical because the senior management responsible for disclosures were not informed of this update.

Violations:

(1) Sections 17(a)(2) and (3) of the Securities Act, which "prohibit any person from directly or indirectly obtaining money or property by means of any untrue statement of a material fact or omission to state a material fact necessary" for the purchaser to make an informed decision;

(2) Section 13(a) and Rules 13a-13 and 12b-20 of the Exchange Act, which require, among other things, issuers to include in quarterly reports to the SEC any material information necessary to make required statements in the filing not misleading;

(3) Section 13a-15(a), which requires issuers to maintain disclosure controls and procedures to ensure timely and accurate filing or submission of required reports under the Exchange Act.

- Blackbaud ordered to pay $3 million civil penalty.

Key Takeaways: Blackbaud decision reflects recent trends of SEC sanctioning a public company for: (1) deficient disclosure of non-financial matters (i.e., cyberattacks); and (2) mischaracterizing risks as "hypothetical" when the company knows otherwise.

Solar Winds

SQUIRE PATTON BOGGS

Key Takeaway: Internal teams should take care to communicate with each other throughout the incident response process to ensure that, among other things, any public representations and statements regarding the incident, including statements to investors, reflect a unified and reasonably accurate information. Timely follow-up statements and notice should be issued as the investigation findings develop.

Change Healthcare

SQUIRE PATTON BOGGS

1. Health payment processing companies in the world (processes over 14 billion transactions annually), targeted in ransomware attack in February 2024.
2. CEO of the parent company testified before Congress and revealed that Change Healthcare failed to implement reasonable security measures, including multi-factor authentication, despite being required by its parent company to do so.

Key Takeaway: Be prepared to address high-scale incidents that accounts for and addresses the risk of business interruption to mitigate the downstream impact of an incident to your customers. In addition, routinely audit whether policies and procedures are being followed.

U.S. Securities and Exchange Commission ("SEC") – Cybersecurity Rules

SQUIRE PATTON BOGGS

May 2024: SEC Statement Clarifying Reporting Required Under Item 1.05 of Form 8-K.

1. Public companies must disclose material cybersecurity incidents under Item 1.05 of Form 8-K, and all other voluntary disclosures (i.e., cybersecurity incidents for which there has not yet been a materiality determination or an immaterial cybersecurity incident the company is voluntarily disclosing) should be submitted under Item 8.01 of Form 8-K. If the company later determines that an incident submitted under Item 8.01 is material, then it must re-submit it under Item 1.05.
2. Guidance is not intended to discourage voluntary reporting of immaterial incidents or early reporting of incidents for which materiality has not been determined. Rather, the SEC simply wants to mitigate the risk of investor confusion and the risk of dilution of the value of an Item 1.05 disclosure.

Cybersecurity Roundup

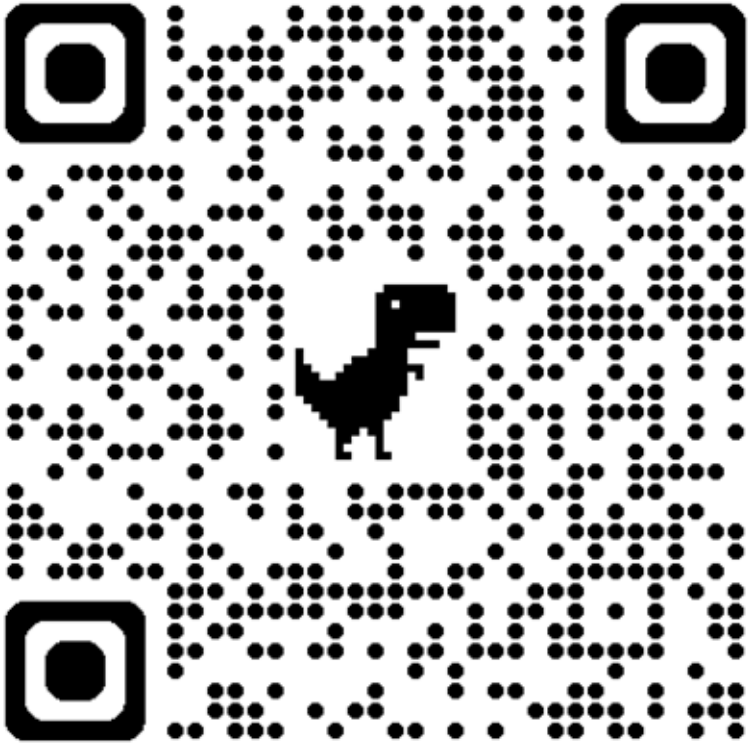
SQUIRE PATTON BOGGS

1. Have an incident response plan in place and have regular tabletop exercises.
2. If you are a publicly traded company, be sure to include in your incident response plan steps on how to assess whether an incident is material, and the process for preparing, reviewing, obtaining internal approvals, and submitting any required reports.
3. If customer data is affected, review your contracts and determine relevant security incident obligations.
4. Include in your response plan a designated communications lead.
5. Identify outside counsel you trust who can help you respond to the incident and prepare for forthcoming litigation and enforcement actions.

SQUIRE PATTON BOGGS

PrivacyWorld

Subscribe Today!



Resources (FTC Consumer Protection and Data Protection):

SQUIRE PATTON BOGGS

(1) Squire's AI Law & Policy Hub, available at https://aihub.squirepattonboggs.com/.
(2) Competition Policy International TechREG Chronicles, "Uncloaking Dark Patters: Identifying, Avoiding, and Minimizing Legal Risk." Available at: https://media.squirepattonboggs.com/pdf/Data-Protection/Uncloaking_Dark_Patterns_Identifying_Avoiding_And_Minimizing_Legal_Risk.pdf
(3) OneTrust Article, "USA: Navigating the maze of direct marketing regulations." Available at: https://www.dataguidance.com/opinion/usa-navigating-maze-direct-marketing-regulations.
(4) Squire Patton Boggs Insights, "Unsubscribed! – FTC Proposes Substantial Amendments to the Negative Option Rule to Cover all Autorenewals, including B2B Services, and Add New Disclosure, Consent, and Cancellation Requirements," available at https://www.squirepattonboggs.com/-/media/files/insights/publications/2023/04/unsubscribed-ftc-proposes-substantial-amendments/unsubscribed_ftc_proposes_substantial_amendments.pdf.
(5) Privacy World, "Health and Health-ish Data and Advertising Under Scrutiny," available at https://www.privacyworld.blog/2023/06/health-and-health-ish-data-and-advertising-under-scrutiny/.
(6) Privacy World, "Sensitive Data Processing is in the FTC's Crosshairs," available at https://www.privacyworld.blog/2024/02/sensitive-data-processing-is-in-the-ftcs-crosshairs/.

Resources (Made in USA and Green Claims Update):

SQUIRE PATTON BOGGS

(1) FTC Press Release, "FTC Issues Rule to Deter Rampant Made in USA Fraud," (July 1, 2021) available at https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-issues-rule-deter-rampant-made-usa-fraud

(2) FTC Business Guidance: "Complying with the Made in USA Standard" (available at https://www.ftc.gov/business-guidance/resources/complying-made-usa-standard)

(3) FTC Press Release, "FTC Action Leads to $2 Million Penalty Against Kubota for False Made in USA Claims," (January 26, 2024), available at https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-action-leads-2-million-penalty-against-kubota-false-made-usa-claims.

(4) FTC Press Release, "Williams-Sonoma Will Pay Record $3.17 Million Civil Penalty for Violating FTC Made in USA Order," (April 26, 2024), available at https://www.ftc.gov/news-events/news/press-releases/2024/04/williams-sonoma-will-pay-record-317-million-civil-penalty-violating-ftc-made-usa-order.

(5) FTC Closing Letter to Rob Canales, CEO & Co-Founder of ROKA Sports, Inc., (May 17, 2024), available at https://www.ftc.gov/system/files/ftc_gov/pdf/2024-05-17-roka-closing-letter.pdf

(6) FTC Maverick Closing Letter, (May 17, 2024), available at https://www.ftc.gov/system/files/ftc_gov/pdf/2024-05-17-maverick-closing-letter.pdf

(7) *Dorris v. Danone Waters of America*, No. 22 Civ. 8717 (NSR), 2024 WL 112843 (S.D.N.Y. Jan. 10, 2024).

(8) Voluntary Carbon Markets Joint Policy Statement and Principles (May 2024), available at https://www.whitehouse.gov/wp-content/uploads/2024/05/VCM-Joint-Policy-Statement-and-Principles.pdf.

Resources (Consumer Dispute Trends and Arbitration Update):

SQUIRE PATTON BOGGS

(1) Squire Patton Boggs Insights, “Updates to Mass Arbitration Rules: Scope and Anticipated Impact”, available at https://www.privacyworld.blog/2024/03/updates-to-mass-arbitration-rules-scope-and-anticipated-impact/

(2) Squire Patton Boggs Insights, “Arbitration Provider JAMS Creates New Mass Arbitration Procedures”, available at https://www.privacyworld.blog/?s=JAMS+mass+arbitration

(3) JAMS Mass Arbitration Procedures and Guidelines, available at https://www.jamsadr.com/mass-arbitration-procedures

(4) AAA Mass Arbitration Supplementary Rules, available at https://www.adr.org/mass-arbitration.

(5) *Greenley v. Kochava*, 2023 WL 4833466 (S.D. Cal. July 27, 2023)

Resources (Cybersecurity):

SQUIRE PATTON BOGGS

(1) Privacy World, “SEC Adopts Final Cybersecurity Risk Management and Incident Disclosure Regulations” (July 2023), available at https://www.privacyworld.blog/2023/07/sec-adopts-final-cybersecurity-risk-management-and-incident-disclosure-regulations/.

(2) Privacy World, “FBI and DOJ Issue Guidance on SEC Incident Reporting Delay Requests” (January 2024), available at https://www.privacyworld.blog/2024/01/fbi-and-doj-issue-guidance-on-sec-incident-reporting-delay-requests/.

(3) SEC Statement: “Disclosure of Cybersecurity Incidents Determined To Be Material and Other Cybersecurity Incidents[*]” (May 21, 2024), available at https://www.sec.gov/news/statement/gerding-cybersecurity-incidents-05212024.