

大成 DENTONS

In-House Counsel CLE Webinar Series: Grow, Protect, Operate and Finance

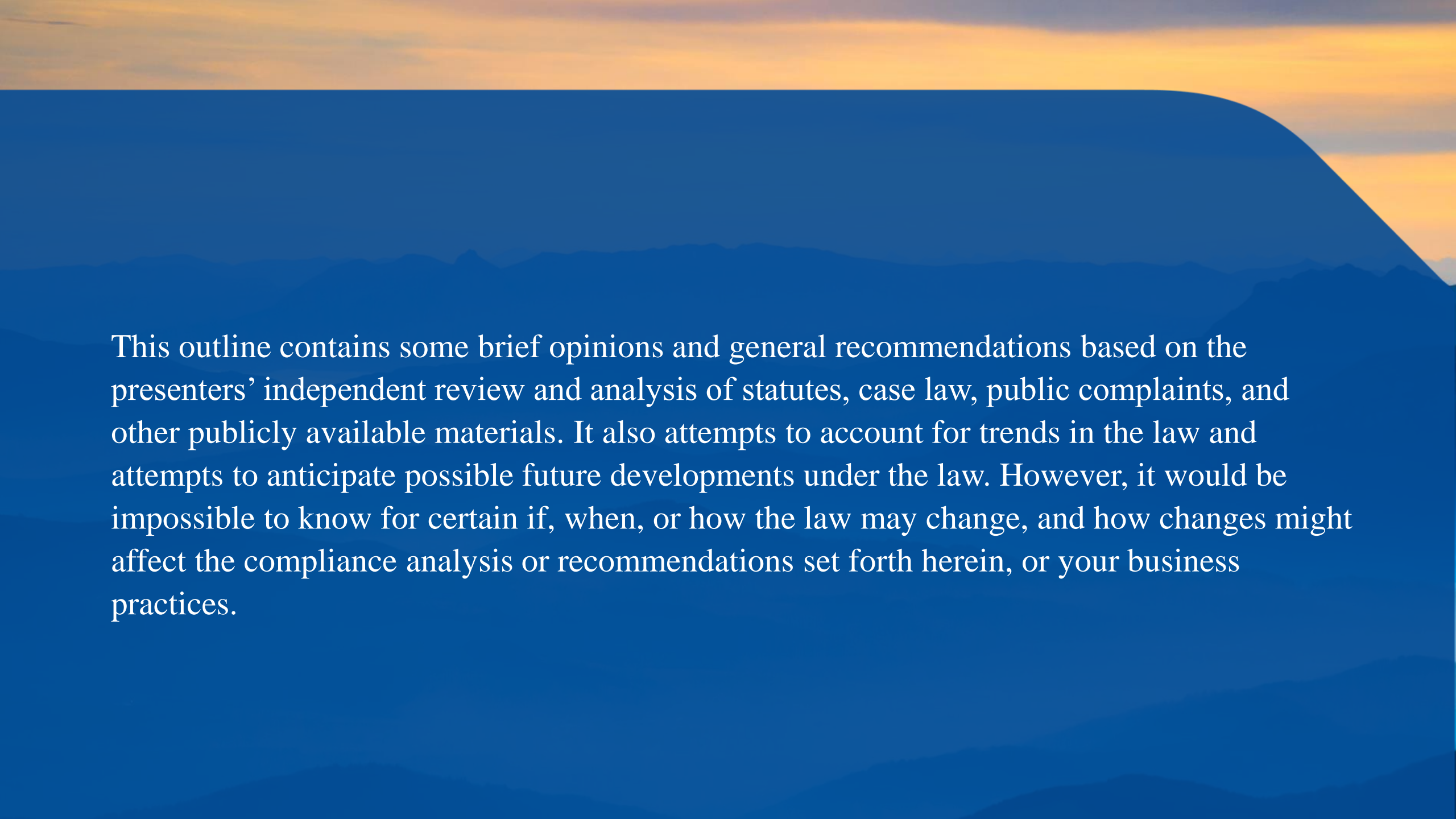
January 19, 2022

Understanding and Protecting Against Common Consumer- Related Claims for Consumer Facing Businesses

Jordan Cameron and Craig Kleinman

This outline provides an overview and some brief analysis regarding a wide variety of Federal marketing laws and regulations. State and criminal laws and regulations may require different compliance standards and obligations than those set forth herein.

It is impossible to provide any promise or guarantee regarding the results of your reliance on this outline or your adherence to the recommendations herein. This outline is intended to be informational and educational only, and is not intended to replace your own research, analysis, and application of the law to facts on a case-by-case basis. The law, regarding consumer matters, especially through digital media, is rapidly changing and dynamic. New opinions, theories of violations, precedent or statutory analyses may develop that have not been considered in the preparation of this outline. It shall be your obligation to remain apprised of all developments in the law that affect your business.



This outline contains some brief opinions and general recommendations based on the presenters' independent review and analysis of statutes, case law, public complaints, and other publicly available materials. It also attempts to account for trends in the law and attempts to anticipate possible future developments under the law. However, it would be impossible to know for certain if, when, or how the law may change, and how changes might affect the compliance analysis or recommendations set forth herein, or your business practices.

Summary

High-level training and recommendations for compliance with marketing and consumer communication compliance, and associated consumer protection laws. The training will provide an overview of FTC Truth in Advertising regulations, the Telephone Consumer Protection Act and the Telemarketing Sales Rule, the CAN-SPAM Act, the American with Disability Act (as its applies to websites), with commentary on similar State laws, with a focus on preventative measures to avoid claims, as well as current Plaintiff strategies.

FTC Truth in Advertising

FTC Act generally - Code Section 15 U.S.C. § 45

“Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.”

Rule Making Authority - The Commission is hereby empowered and directed to prevent . . . unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.”

The Ultimate Question

As advertised...



...in reality



Whether or not the advertising has a tendency or capacity to be false or deceptive.

Types of Claims

- a. Monadic Claims – Claims touting the alleged benefits of the product itself, based on its own attributes, without comparisons to another product.
- b. Comparison Claims – Claims that compare Advertiser's product to other products.
- c. Third Party Claims – Any advertising message that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser.
- d. Establishment Claims – Claims proved by competent and reliable testing.

The “Reasonable Consumer”

The typical person looking at the ad. The analysis considers all possible meanings that can be gleaned from the ad: express or implied – the Commission examines **“the entire mosaic, rather than each tiles separately.”**

A “Reasonable Consumer” standard is applies to determine deception and unfairness.



Deception

An advertisement or marketing practice is deceptive if there is a representation, omission of information or some other practice that is likely to mislead a reasonable consumer and which is likely to influence or otherwise “affect the consumer’s conduct or decision with regard to a product or service,” to that customer’s detriment.



In a nut shell:

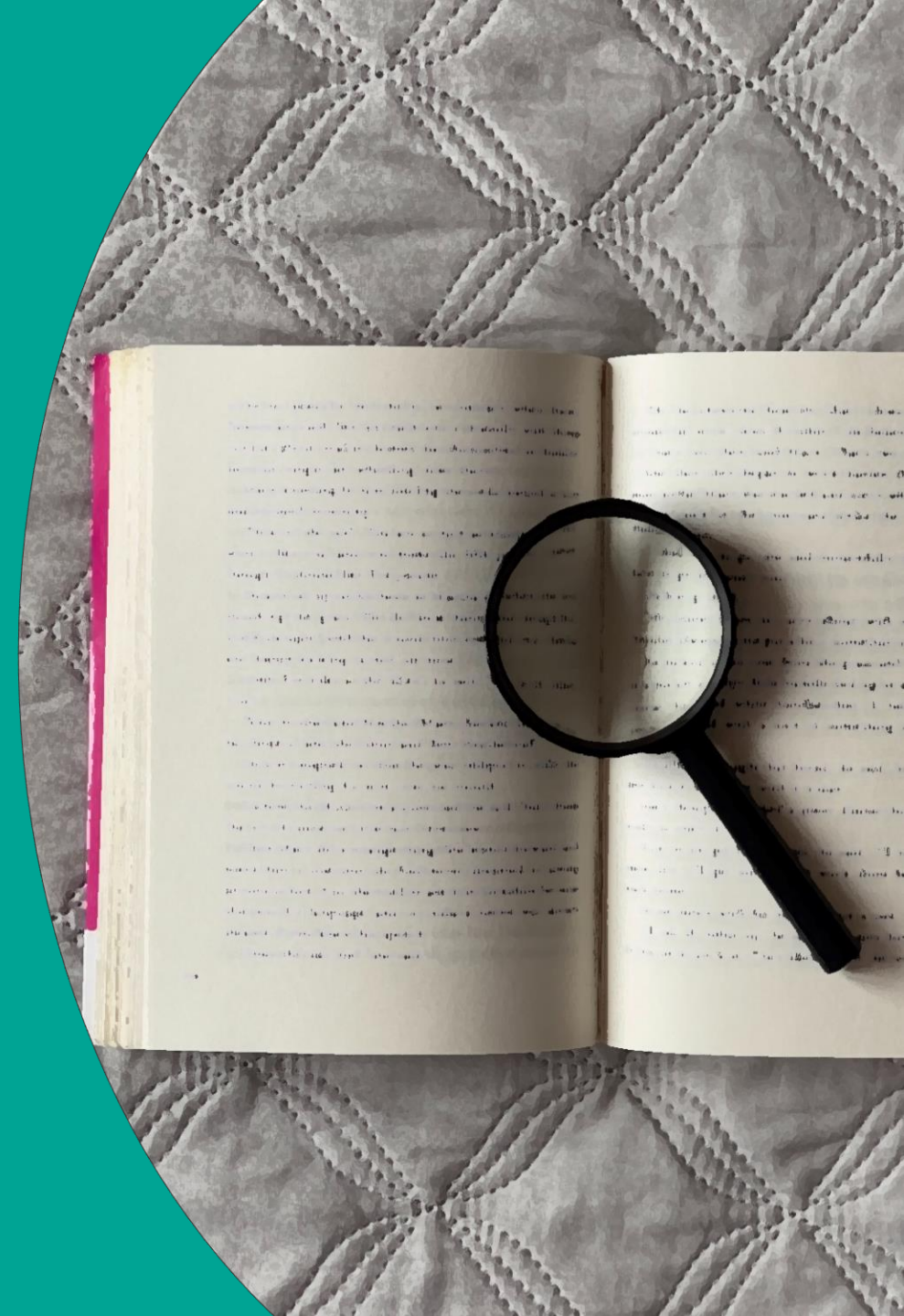
- Advertising must be truthful and non-deceptive;
- Advertisers must have evidence to back up their claims;
- and
- Advertisements cannot be unfair.

A claim can be literally true, but if it is only true in limited circumstances, or if it is subject to more than one interpretation, one of which is not true, or misleading in its overall effect, it may be deceptive.

Notes on Disclosures:

Accurate information in a footnote or text will likely not remedy a false headline because consumers may glance only at the headline.

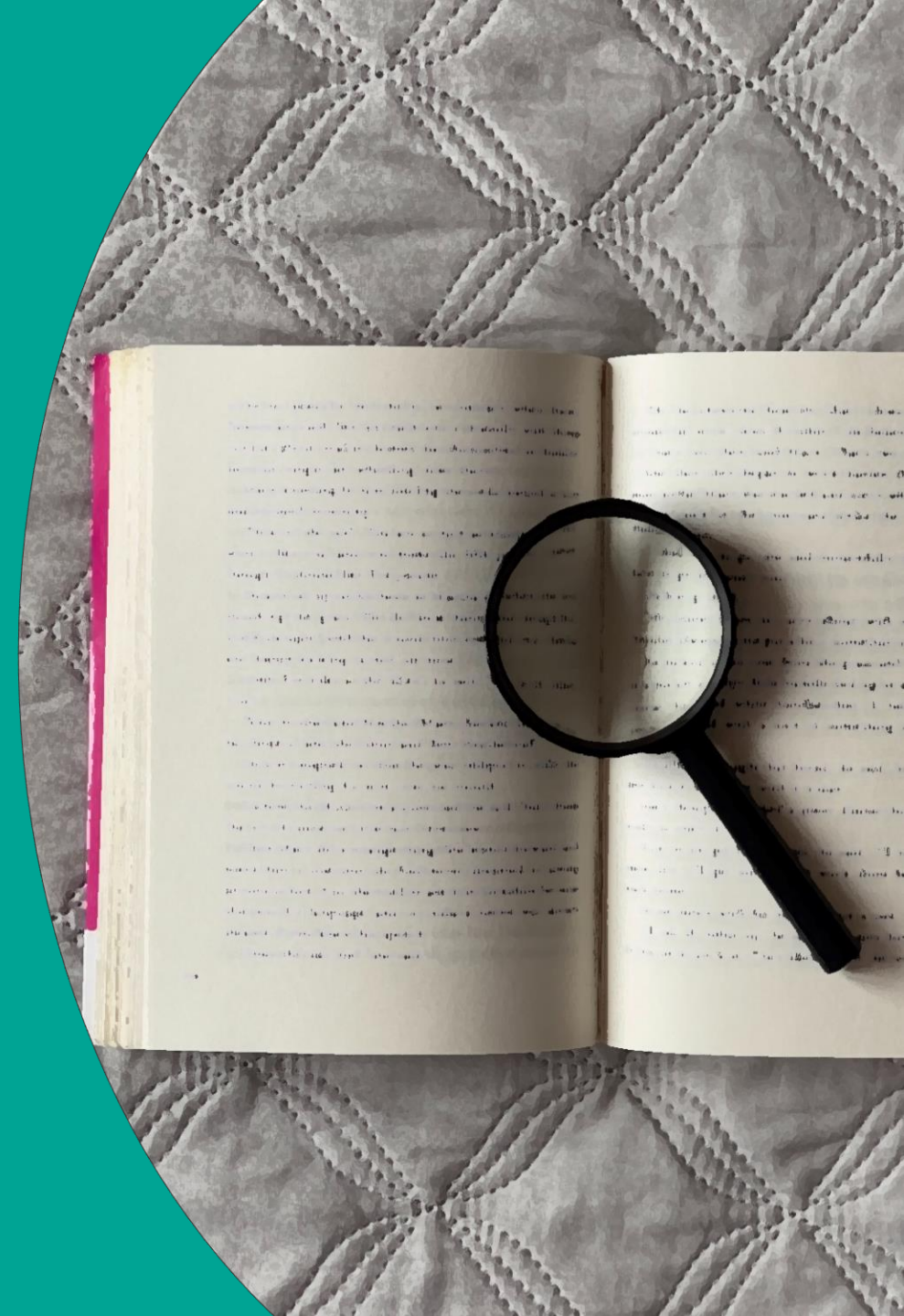
Clear and conspicuous – “readable [or audible] and understandable to a reasonable consumer.”



Disclosures:

In evaluating disclosures, factors include the four Ps:

- Prominence
- Presentation
- Placement
- Proximity



Unfairness

The principal focus of the Commission's unfairness policy is to **protect consumer sovereignty by attacking practices that impede consumers' ability to make informed choices.**





An act or practice is “unfair” if it satisfies three factors:

1. Causes or is likely to cause substantial injury to consumers;
2. The injury is not reasonably avoidable by consumers;
3. The injury is not outweighed by countervailing benefits to consumers or to competition.

Substantiation

Simply, must have evidence/
support to back-up claim.

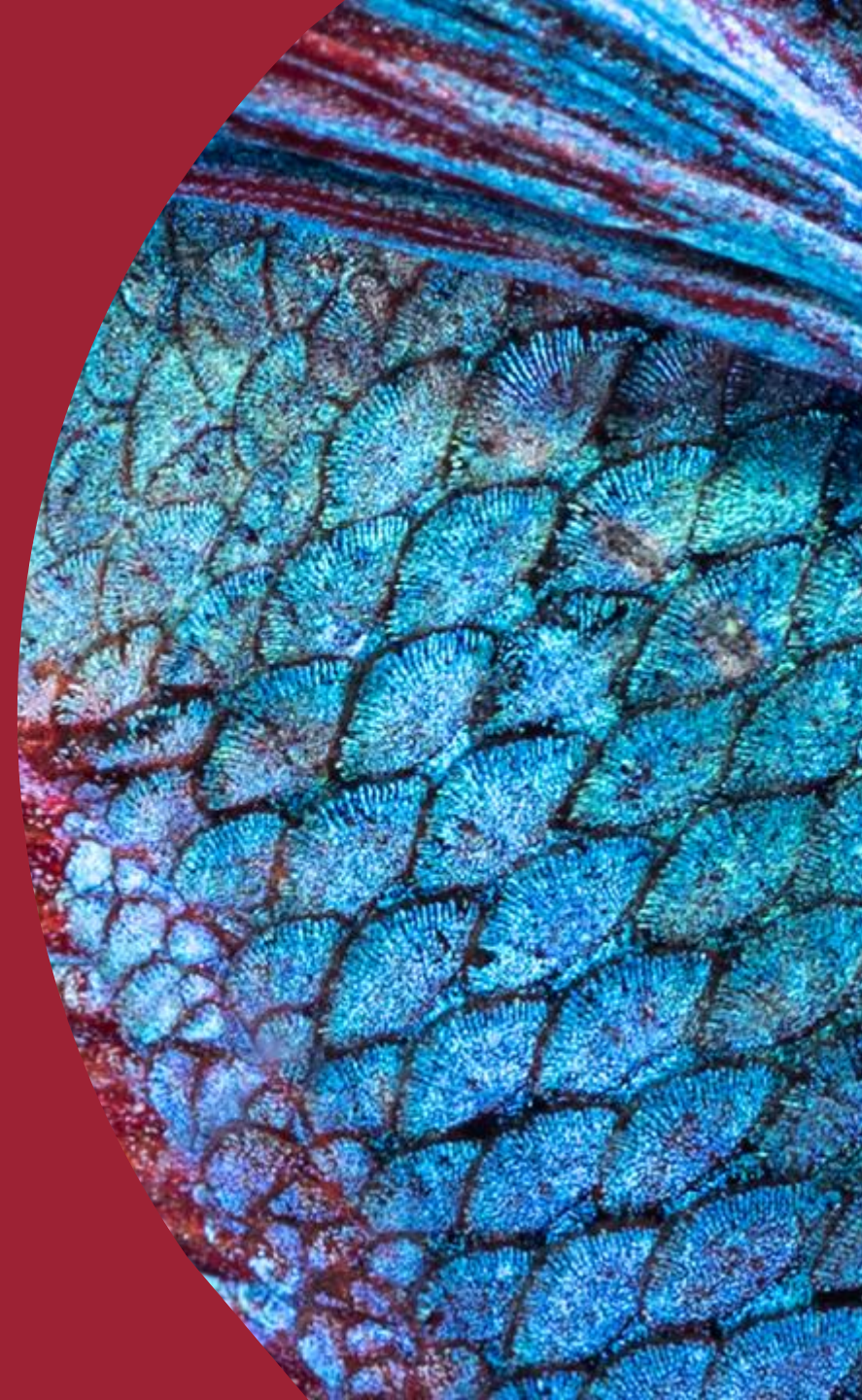
An advertiser must possess at
least the level of substantiation
expressly or impliedly claimed in
the ad.

- Clinically tested
- Doctor approved
- Mom's favorite?



If no specific level of substantiation is claimed, a reasonable basis is determined on a case-by-case basis by analyzing six “Pfizer factors.”

1. the type of claim;
2. the benefits if the claim is true;
3. the consequences if the claim is false;
4. the ease and cost of developing substantiation for the claim;
5. the type of product; and
6. the level of substantiation experts in the field would agree is reasonable.



Health and Safety Claims

“competent and reliable scientific evidence,” typically defined as “tests, analyses, research, studies, or other evidence based upon the expertise of professionals in the relevant area, that has been conducted and evaluated in an objective manner by persons qualified to do so, using procedures generally accepted in the profession to yield accurate and reliable results.”

Influencers and endorses
beware: Others can't say what
Company can't substantiate.





Special Claims

Typically require heightened and specific substantiation.

Typically have special FTC Policy Statements. If not, look to Commission decisions, opinion letters, and case law.

Example – Made in USA (standards derived from Policy Statement, Commission Opinions, and case law)

The product has been last “**substantially transformed**” in the United States.

Some factors to consider in the analysis:

1. Whether the key raw material is foreign or domestic.
2. Percentage of foreign content, if any.
3. How far removed foreign materials are from finished product.
4. Percentage of cost of the product manufacturing in the USA and foreign.
5. Whether claims are qualified in some way (e.g. Made in USA of domestic and foreign materials)



Enforcement/Liabilities/Penalties

Strict Liability (False or Unsubstantiated Claims)

The advertiser is strictly liable for violations of the FTC Act. Neither proof of intent to convey a deceptive claim nor evidence that consumers have actually been misled is required for a finding of liability.

Individual Liability (False or Unsubstantiated Claims)

Corporate officers/control persons may be held individually liable for violations of the FTC Act if the officer “owned, dominated and managed” the company and if naming the officer individually is necessary for the order to be fully effective in preventing the subject deceptive practices.

Individual liability is justified “where an executive officer of the respondent company is found to have personally participated in or controlled the challenged acts or practices” or if the officer held a “control position” over employees who committed illegal acts.

Consumer/Competitors – No private right of action under FTC Act, but ... Lanham Act Section 43 (15 USC 1125).

Any person who, on or in connection with any goods or services, or any container for goods, uses in commerce any word, term, name, symbol, or device, or any combination thereof, or any false designation of origin, false or misleading description of fact, or false or misleading representation of fact, which –

- is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person, or
- in commercial advertising or promotion, misrepresents the nature, characteristics, qualities, or geographic origin of his or her or another person's goods, services, or commercial activities,
- shall be liable in a civil action by any person who believes that he or she is or is likely to be damaged by such act.

Damages include: (1) defendant's profits, (2) any damages sustained by the plaintiff, and (3) the costs of the action. In assessing damages the court may enter judgment, according to the circumstances of the case, for any sum above the found as actual damages, not exceeding three times such amount. In exceptional cases may award reasonable attorney fees to the prevailing party.



FTC – The Commission is empowered and directed to prevent persons, partnerships, or corporations from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce. (15 USC 45)



Cease and Desist – In advertising cases, the basic administrative remedy is a cease and desist order. The purpose of the order is two-fold:

1. enjoin the conduct alleged in the complaint; and
2. to prevent future violations of the law.



Fencing in – The Supreme Court has afforded the Commission broad discretion in fashioning fencing-in provisions that will not be disturbed except “where the remedy selected has no reasonable relation to the unlawful practices found to exist.”



Corrective Advertising/ Disclosures/Notifications.

Bans (i.e., from certain businesses or certain actions).

Name excision (if name is part of consumer confusion).

Financial Remedies (Disgorgement, Restitution, Sanctions).

- Up to \$43,792 per violation. 16 CFR § 1.98

Attorney General – May proceed in civil action against violators of Commission orders. May seek damages of not more than \$10,000 per violation.

How to protect

- a. Know the law
- b. Know how the law applies to your business practices
- c. Know the process
- d. Written marketing policies
- e. Contracts/indemnity
- f. Substantiation file
- g. Dynamic approved claims list
- h. Communication between legal/marketing

**Telephone Consumer
Protection Act (“TCPA” – 47
U.S.C. § 227) and
Telemarketing Sales Rule
 (“TSR” – 16 CFR 310)**



TCPA Generally – With few exceptions, the Telephone Consumer Protection Act prohibits autodialed calls or text messages and prerecorded calls, unless made with the prior express consent of the called party.

- a. Prior express written consent is required for telephonic communications that includes or introduces an advertisement.
- b. Restrictions on making autodialed calls to cell phones encompass both voice calls and texts. Just as texts are a subset of “calls”, “robotexts” are a subset of “robocalls” or autodialed calls.
- c. May rely on consent for up to 18 months, unless terminated.

TSR Generally - The Telemarketing Sales Rule is similar to TCPA and requires telemarketers to make specific disclosures of material information; prohibits misrepresentations; sets limits on the times telemarketers may call consumers; prohibits calls to a consumer who has asked not to be called; and sets payment restrictions for the sale of certain goods and services.



General Requirements:

- Misrepresentations, profanity, obscene language, etc. of any nature are prohibited;
- Must disconnect unanswered calls within 15 seconds or 4 rings.
- Must scrub against National Do Not Call every 30 days, and do not place any calls to any number on the list unless and exception applies.
- Must not call outside of the hours of 8 a.m. and 9 p.m. based on the location of the recipient.
- Must not block ID of caller from the recipient's caller-ID.
- Must not spoof a local number.

Protective Measures

- a. Know the law
- b. Know how the law applies to your business practices
- c. Double opt-in for mobile consent
- d. Maintain Internal Do Not Call List
- e. Third party scrub
- f. Written Policies/Training
- g. Enforce you policies
- h. Only trusted sources for leads



Establish proper written consent mode

- a. Be in writing
- b. Identify the Advertiser and all companies that will have access to the consumer's phone number;
- c. Make clear the type of Telephonic Communication the consumer is signing up for (consenting to event updates is not the same as consenting to ads);
- d. State that standard messaging fees may apply;
- e. Include how the consumer can opt out at any time;
- f. Disclose that the consumer is not required to provide consent as a condition of purchasing products or services;
- g. Indicate a clear and affirmative agreement (i.e., I agree/ consent);
- h. Obtain the consumer's signature (either electronically through E-SIGN or handwritten).

State registration requirements

The following states have statutes which require a license or registration before telemarketing in that state unless an state exception applies:

Alabama, Alaska, Arizona, Arkansas, California, Colorado, Delaware, Florida, Idaho, Indiana, Kentucky, Mississippi, Montana, Nevada, New Hampshire, New Jersey, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Texas, Utah, Vermont, Washington, West Virginia, Wisconsin, and Wyoming.



Enforcement/Liabilities/Penalties (TCPA)

- Consumer/Attorney General Enforcement
- TCPA violations are assessed on a per-call basis. The standard maximum fine is \$500-per-violation.
- If a court finds that the defendant willfully or knowingly committed TCPA violations, the damages can be assessed at three times their normal amount.
- Class Action

Enforcement/Liabilities/Penalties (TSR)

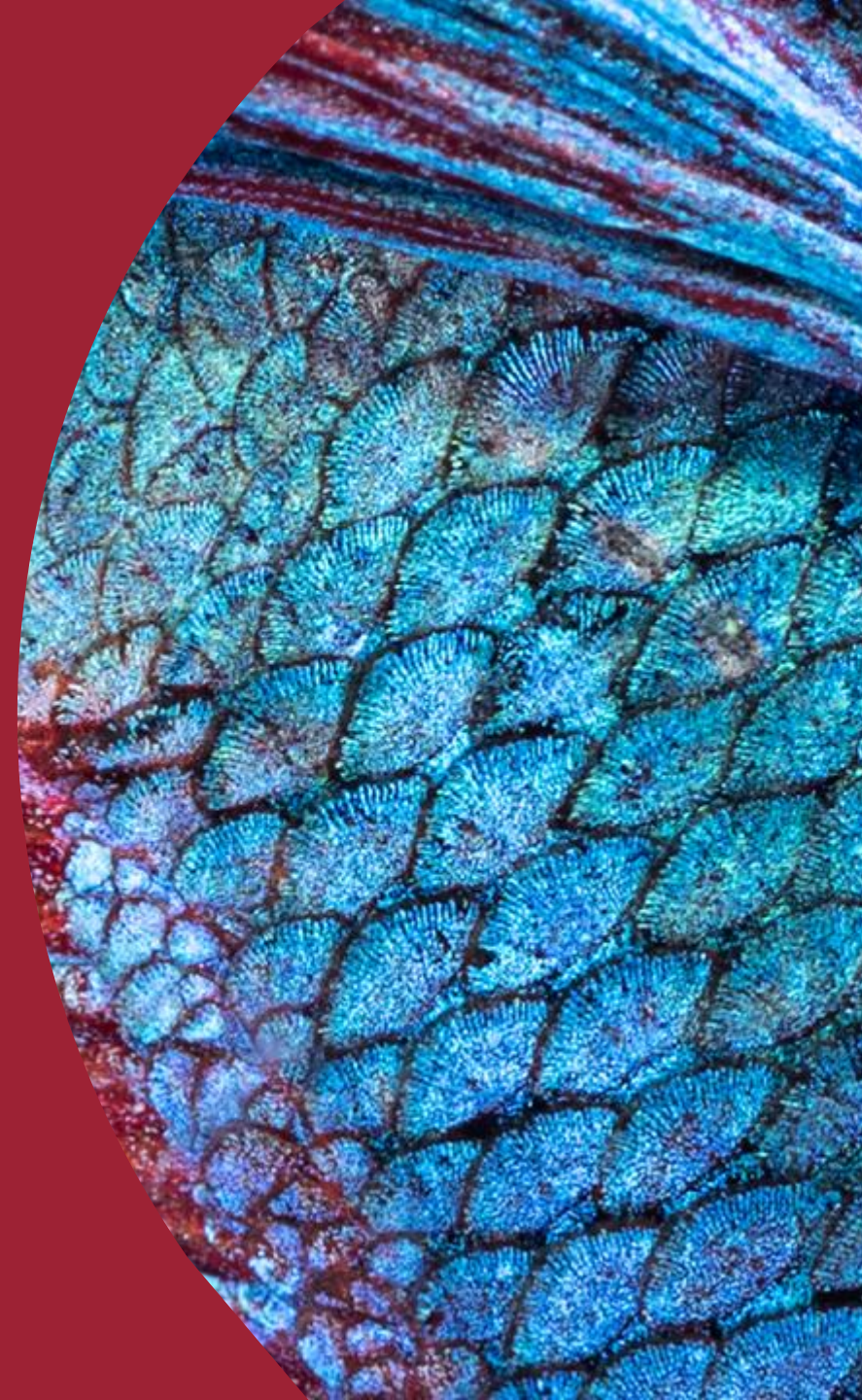
- Enforced by FTC
- Because violations of the TSR are also violations of the Section 5 of the FTC Act, 15 U.S.C. § 45, per call damages can reach \$43,792. 16 CFR § 1.98, plus other non-monetary penalties.

**Controlling the Assault of
Non-Solicited
Pornography and
Marketing Act (CAN-SPAM
– 15 U.S.C. § 7701 et. Seq.)**



General Overview

- Not an opt-in law, like TCPA. Free to email, so long as you follow the rules.
- Misnomer - Not limited to pornography, not limited to non-solicited marketing messages.
- Prohibits sending email (whether solicited or not) with header information that is materially false or materially misleading



Header Violations - Headers may be misleading in the following ways:

1. Spoofed domains.
2. Unregistered domains.
3. False WHOIS registration information.
4. Sending emails from domains obtained in violation of registrar policies.
5. Generic “from” names accompanied by domains with private or cloaked WHOIS information.



Other Violations

1. No deceptive subject headings.
2. Sexually explicit emails by requiring Notices in subject headings.
3. No continued emailing more than ten days after a recipient opts-out.



Content Requirements

Requires the inclusion of certain content in commercial emails.

1. Opt-out Notice and Mechanism
2. Physical Address of “sender” (typically the advertiser)
3. Advertisement Notice (unless the recipient opted-in)

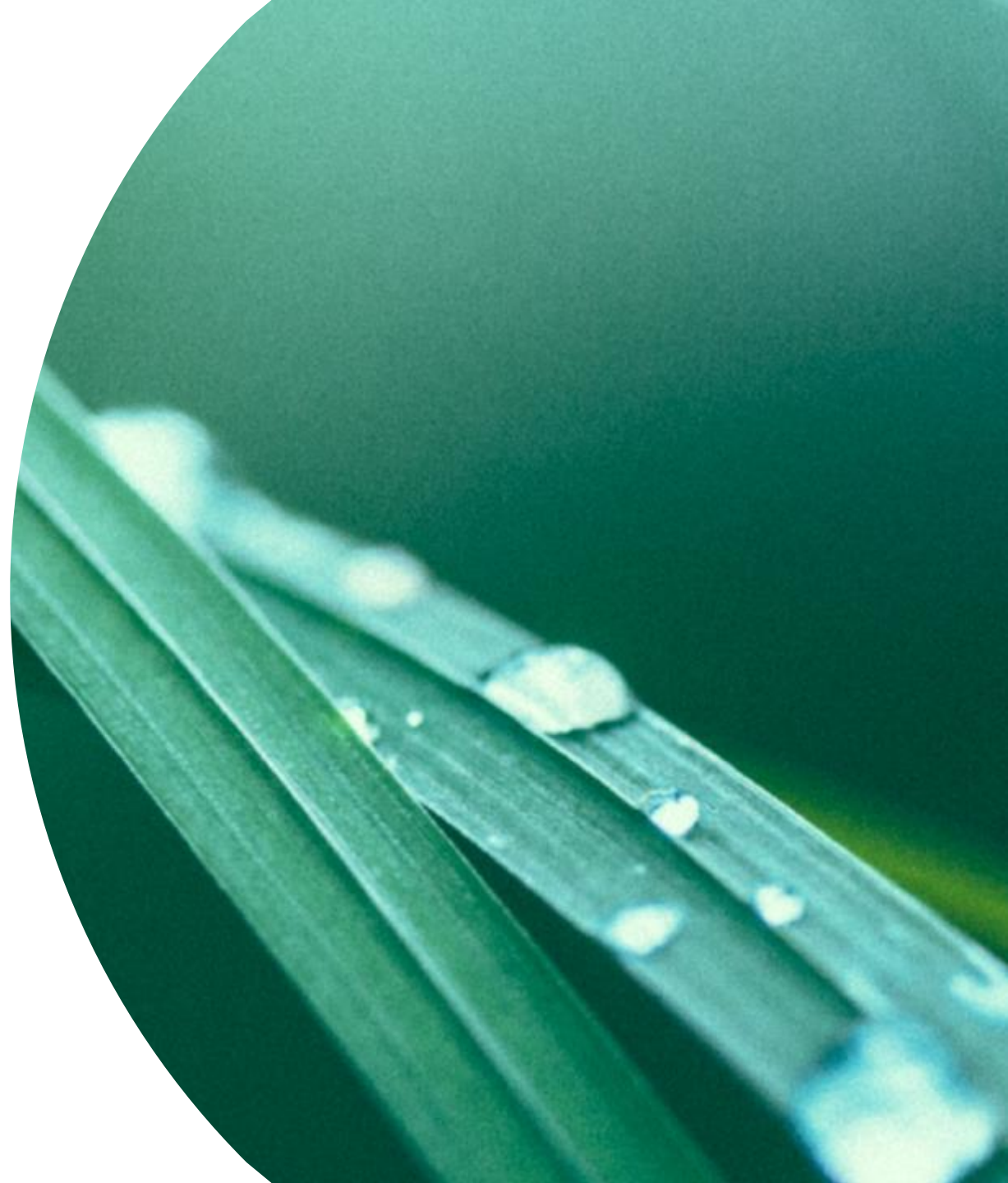
Protective Measures

- a. Know the law
- b. Know how the law applies to your business practices
- c. Written Compliance Policy
- d. Enforce your policy
- e. Contract Protections
- f. Choose affiliates wisely and after due diligence
- g. Maintain internal email suppression list.

Enforcement/Liabilities/Penalties

- Actions may be brought by FTC, Attorney General, Private Internet Access Service (ISP, ESP, Social Media, University - Some combination of physical and technical)
- While the regulation regarding header information creates a violation of CAN-SPAM on a per instance basis, the majority of the other CAN-SPAM regulations require a plaintiff to demonstrate a “pattern or practice” of violating CAN-SPAM.
- CAN-SPAM dictates a statutory damage amount on a per violation basis with certain limitations (up to \$100 per header violations, up to \$25 per other violations).

**Americans with
Disabilities Act** (ADA – 42
U.S.C. § 12181 et seq.)





Section 302 of Title III of the ADA

No individual shall be discriminated against on the basis of disability in the full and equal enjoyment of the goods, **services**, facilities, privileges, advantages, or accommodations of any place of **public accommodation** by any person who owns, leases (or leases to), or operates a place of public accommodation.

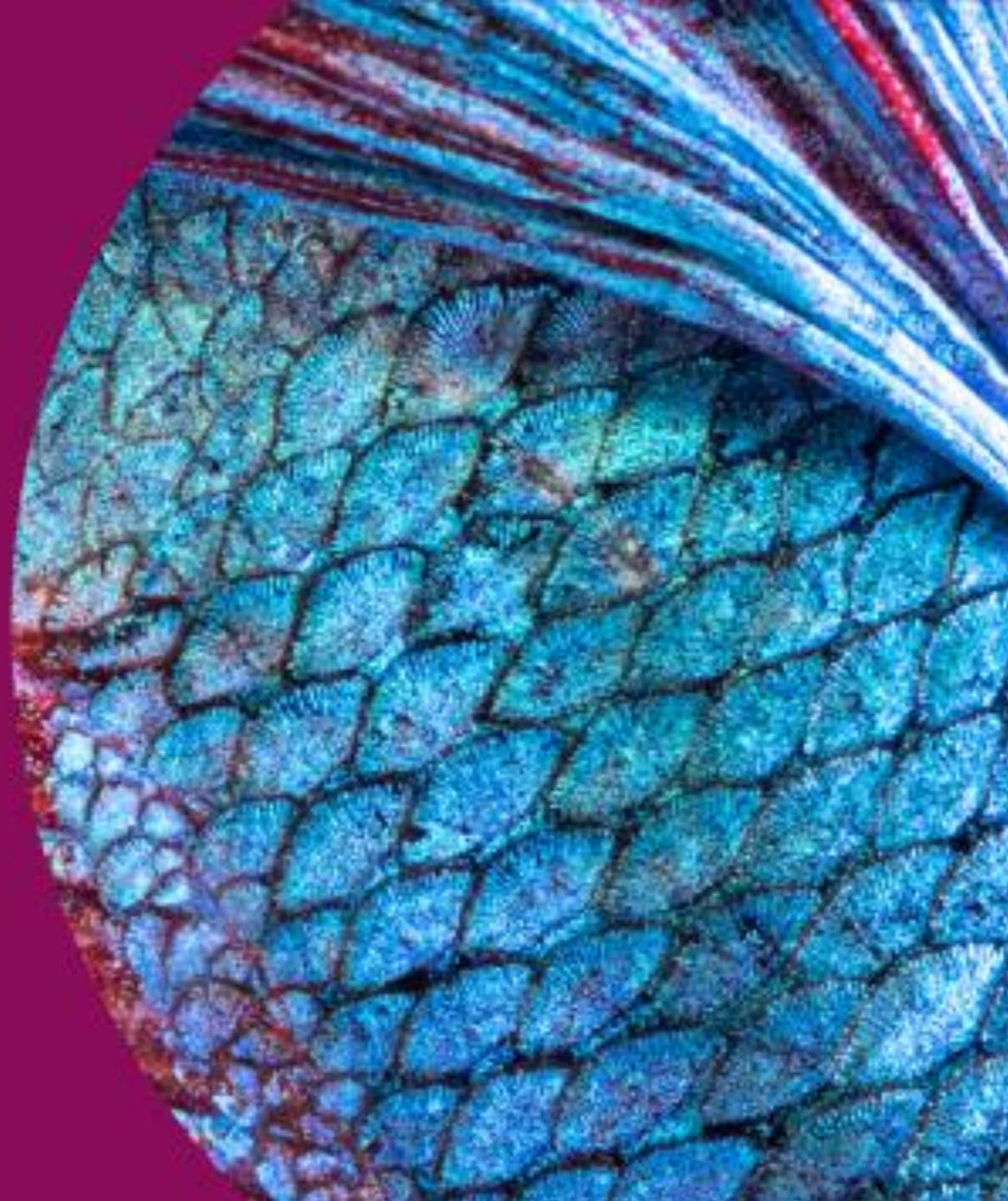
Primary allegations

- A Website is a public accommodation as service that is offered to the general public
- The website is not compatible with screen reader technology (Web Content Accessibility Guidelines (“WCAG”) standards)



Enforcement/ Liabilities/Penalties

- Private Parties – Courts have allowed cases brought by “testers.”
- Injunctions
- Compensatory Damages
- Attorney’s fees



Protective Measures

- a. Know the law
- b. Know how the law applies to your business practices
- c. Accessibility Policy
- d. WCAG 2.1 standards
- e. Test, test, test

Thank you!

Jordan Cameron

jordan.cameron@dentons.com

Craig Kleinman

craig.k@purple.com

大成 DENTONS

SIROTE

Working Remotely: Legal Ethics & Technology Scams

J.S. “Chris” Christie





**J.S. "Chris" Christie
Of Counsel**

+1 205 930 5751
Chris.christie@dentons.com

J.S. "Chris" Christie practices in Dentons Sirote PC's Litigation Practice Group, based in Birmingham, Alabama. He frequently speaks and publishes on employee benefits, health care law, legal ethics, and trial techniques.

In employee benefits litigation, Chris represents plans, fiduciaries, and insurers in ERISA cases and in governmental plan cases. He has tried several ERISA fiduciary breach trials. Since 2012, he has been a Fellow with the American College of Employee Benefits Counsel.

In healthcare litigation, Chris primarily represents hospitals, physicians and other providers and has represented insurers, HMOs and other managed care organizations. For healthcare clients, he has won two healthcare civil False Claims Act trials prosecuted by the Department of Justice.

Normal Lawyer Technology Risks

One example of normal technology risks:

- January 2020, Maze hackers attacked many law firms – South Dakota, Oregon, Texas
- Stole and encrypted data
- One firm, 200 bitcoin ransom
100 delete and 100 allow access (+\$900,000)

Are you next?

While Working Remotely

- **Lawyers' technology risks while working remotely**
- **Computer security at home is not as good**
- **Remote access creates security risks**
- **Lawyers may not be as careful at home**
- **Lawyers' supervising others is more difficult**
- **Scammers expected to increase efforts**

While Working Remotely (cont.)

Remote: same ethical duties, increased technology risks

Why is avoiding technology scams a legal ethics issue?

What are lawyers' ethical duties while working remotely?

Competence

Confidentiality

Supervision

How manage technology risks? Listen, see handout

Legal Ethics and Technology

- **ABA 2012 Model Rules Technology Amendments**
- **Lawyers' Responsibility for Others**
- **ABA Formal Op. 498, 495, 483 & 477R**
- **Practical Considerations for Lawyers**
 - phishing emails**
 - ransomware attacks**
 - computer security**

ABA Commission on Ethics 20/20

- **2012 ABA amended Model Rules based on Commission's technology recommendations**
- **40 States have adopted all or most amendments**
- **10 States have not adopted (including AL)**
- **ABA 2012 Model Rule Amendments highlight what lawyers should consider as to today's technology risks**
- **Not understand technology risks? Embarrassed, worse**

2012 Model Rule Amendments

Model Rule 1.1 (Competence)

- Comment [6] amended (now Comment 8)
- Added phrase beginning with “including”

“a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology” (emphasis added)

2012 Model Rule Amendments (cont.)

Model Rule 1.6 (Confidentiality of Information)

- New Model Rule 1.6(c) added

“(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information regarding the representation of a client.”

2012 Model Rule Amendments (cont.)

Model Rule 1.6, old Comment [16] amended (now [18])

Requires “reasonable” efforts; 5 factors to consider:

- information’s sensitivity
- disclosure likelihood without safeguards
- additional safeguards’ cost
- difficulty implementing safeguards
- extent safeguard makes representing clients difficult

Factors highlight tradeoffs and judgments required



www.dilbert.com scottadams@aol.com

10-4-07 ©2007 Scott Adams, Inc./Dist. by UFS, Inc.

2012 Model Rule Amendments (cont.)

Model Rule 1.6 Comment [17] amended (now [19]) adds
“Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these rules.”

Federal: HIPAA, GLB (Graham-Leach-Bliley Act)

State: Alabama Data Breach Notification Act of 2018

2012 Model Rule Amendments (cont.)

Model Rule 1.4 (communicating with clients)

Amended Comment [4]

- Old Comment [4] required lawyer promptly to return or acknowledge “telephone calls”
- Amended Comment [4] requires a lawyer to “promptly respond to or acknowledge client communications”

Duty to respond to client communications promptly

2012 Model Rule Amendments

Model Rule 4.4(b) (inadvertently sent confidential information)

- **Notice required when lawyer finds documents that were inadvertently sent**
 - **amended to clarify documents = paper, ESI**
- **“inadvertently sent” defined (Comment [2])**
 - **amended to clarify when notice required**

ABA Avoided Metadata Issue

Rule 4.4 amendment avoided ethics op. metadata split:

- **Only with consent or court authority or**
- **No consent or court authority required**

Ala. Formal Op. 2007-02: lawyer must

- **send documents with reasonable care**
- **must not mine documents for metadata**
- **if know metadata inadvertently sent, must notify**

Model Rule of Professional Conduct 5.1

Responsibilities of a Partner or Supervisory Lawyer

(a) A partner in a law firm . . . shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

(b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct. . . .

Model Rule of Professional Conduct 5.3

Responsibilities Regarding Nonlawyer Assistance

With respect to a nonlawyer employed or retained by or associated with a lawyer:

- (a) A partner . . . shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
- (b) A lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; . . .

ABA Formal Op. 498 (Mar. 10, 2021)

Virtual Practice

- Virtual practice is remote technologically enabled law practice
- If follow Rules, lawyer's practicing virtually is permissible
- Rule 5.5 (unauthorized practice of law) see ABA Formal Op. 495
- Rules 1.1 (competence), 1.3 (diligence), 1.4 (communication), 1.6 (confidentiality)
- Rules 5.2 (supervising other lawyers), 5.3 (supervising nonlawyers)

ABA Formal Op. 495 (12/16/2020)

Lawyers Working Remotely

Model Rule 5.5(a) prohibits unauthorized practice of law

Lawyers can work remotely in different jurisdiction if

- do not establish an office or other systematic presence
- do not “hold out” a presence or availability there
- do not actually provide legal services in that local jurisdiction, unless otherwise authorized

ABA Formal Op. 483 (10/17/2018)

Lawyers' Obligations After an Electronic Data Breach or Cyberattack

“Data breaches and cyber threats . . . are a major professional responsibility.”

Model Rule 1.1 – Competence

Model Rule 1.6 – Confidentiality

Model Rule 5.1 – Supervising other lawyers

Model Rule 5.3 – Supervising staff

ABA Formal Op. 483 (10/17/2018) (cont.)

Lawyers' Obligations After a Data Breach or Cyberattack

- **Follow data breach plan developed before breach**
- **Must monitor for data breach**
- **Stop breach and restore systems**
- **Reasonably determine what occurred**
- **Provide notice of data breach to clients**
- **Notice must give sufficient information**

ABA Formal Op. 477R (5/21/2017)

Securing Communication of Protected Client Information

- Reviews 2012 Model Rules Technology Amendments
- Duty to prevent inadvertent or unauthorized disclosures
- Reasonable efforts standard (safeguards)
(sensitivity, likelihood, cost, difficulty, ease to use)
- Special protections by agreement, law or circumstances

Practical Cybersecurity Considerations

- **Avoid Phishing Email Scams**
- **Avoid, Respond to Ransomware Attacks**
- **Other Computer Security Issues**
 - **Remote access risks**
 - **Password Fundamentals**
 - **Mobile Device Security**
 - **Wi-Fi Interception**
 - **Videoconferencing**

Avoiding Technology Scams

- **Computer “hacked” usually means user allowed access**
- **Risks of being hacked or scammed created by**
 - **Allowing remote access to computer system**
 - **Responding to phishing and spoofing emails**
 - **Downloading software (games or apps) with malware**
 - **Downloading malware by opening email attachment, infected thumb drive, or questionable websites**
- **Malware can record keystrokes, encrypt data, lock system**

Avoiding Phishing Scams



Your fedex.com e-mail address

fedex.com

Account Requires Complete Profile Update, We have recently detected that different computer user had attempted gaining access to your Online account, and multiple password was attempted with your user ID. It is now necessary to re-confirm your account information to us. If this process is not completed within 24-48 hours. We will be forced to suspend your Account Online Access as it may have been used for fraudulent purposes.

Please update profile immediately by following this link.

[Click Here](#)

Thank you for using fedex.

Sincerely, FedEx Online Customer Care.



PSG Spear Phishing Email

To: Lee Controller
From: Josh Executive
Re: Urgent Fund Transfer

We have been working secretly on a key acquisition. Please wire the agreed \$1.7 million as soon as possible. For wire transfer details, give full attention to attorney Mike Leach.

Treat this matter with the utmost discretion and deal solely with Leach.

PSG, LLC v. Ironshore Indemnity, Inc.

Scammers spear phished PSG controller

- “Leach” telephoned with wire instructions
- Wells Fargo asked PSG to verify
- Controller confirmed with “Leach”
- Wells Fargo released the hold
- \$1.7 million wired 2 hours after email
- PSG had cyber insurance policy
- Policy covered “fraudulent instruction” loss
- Insurer had denied claim as not “direct loss”
- 11th Cir. affirmed summary judgment for PSG

Avoid Being a Caught Phish?

Spear phishing scam (like PSG case)

Email Red Flags – learn, train, test:

- **Purports to be from authority (IRS, court, boss)**
- **Urges quick response**
- **Insists on internal secrecy**
- **Involves transfer of money**
- **Requests using new payment instructions**

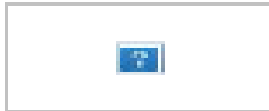
American Tooling Center v. Travelers

- Imposter sent email to insured, posing as insured's vendor
- Imposter requested insured to change payment instructions
- Insured paid vendor's invoices into imposter's account
- District Court ruled that scam was not "computer fraud"
- 6th Circuit entered over \$500,000 judgment for Insured
- 5th Circuit reached opposite result in similar case

Confirm changes to payment instructions with trusted person

From: American Express <ourtime3@frontier.com>
Sent: Monday, February 3, 2020 8:05 AM
To: Christie, Chris <cchristie@sirote.com>
Subject: Approval

This message originated from outside Sirote & Permutt, P.C.



ACCOUNT ENDING: XXXX

Dear Member, Account Security Update

This email is to notify you that you have a new payment pending on your American Express account

For safety reasons, The new incoming payment has been placed on hold. Update of your account is required as a means to accept the new payment.

Kindly click on the link below to update and approve your payment.

[Approve Your Payments Now](#)

[Questions? Let's chat](#)



[PRIVACY STATEMENT](#) | [UPDATE YOUR EMAIL](#)

Your account information is included above to help you recognize this as a customer care e-mail from American Express. To learn more about e-mail security or report a suspicious e-mail, please visit us at americanexpress.com/phishing. We kindly ask you not to reply to this e-mail but instead contact us via [Customer Care](#).

Â© 2019 American Express. All rights reserved.

AGNEUSPK0007001



Avoid Being a Caught Phish? (cont.)

Other phishing scam red flags (learn, train, test):

- Suspicious email sender address
- Requests personal info (e.g., account ##)
- Generic, incorrect name in greeting
- Requests clicking on suspicious URL links
- Offers award if open or click
- Requests to download file
- Asks for log-in and password

Corona Virus Phishing Scams

Prof. Gary Warner, UAB Criminal Justice Dept.:

New junk email scams, same methods

- **Email example he discussed had Fox News logo**
- **Selling virus cures or masks, fake charities**
- **SBA Loans, \$600 unemployment, \$1200 stimulus**
- **Fill out form: private information, malware**

DCH Ransomware Attack

DCH = 3 hospitals (583 + 204 + 61 beds)

- **10/1/2019 attack discovered**
- **Contacted law enforcement, IT & forensic**
- **Computer systems shut down for weeks**
 - **Paper medical records only**
 - **Transferred, diverted patients**
- **Paid attacker ransom for decryption key**
- **Calls falsely claiming to be from DCH**

Daniels v. DCH Healthcare System

- **Filed N.D. Ala. (Dec. 2019)**
- **Negligence, contract, fiduciary duty claims**
- **Class damages and equitable relief**
 - **Forgone medical care**
 - **Sought alternative care**
 - **Identities at risk**
- **Dismissed about 120 days after filed**

Avoid Ransomware Attack? Don'ts

- Don't open risky emails or attachments
- Don't click on risky URL links
- Don't download games, non-work apps
- Don't open risky thumb drives or CDs
- Don't visit suspicious or fake websites
- Don't respond to “urgent” requests
- Don't trust telephone caller ID
- Don't (never) reply with password

Avoid Ransomware Attack? Do's

- **Block unsafe, suspicious or fake websites**
- **Check suspicious URL addresses**
- **Install anti-virus, security software**
- **Update all types of software**
- **Replace software not updated**
- **Separate work and personal computer use**
- **Backup files in remote, unconnected place**
- **Train and test lawyers and staff**
- **Use common sense**

Respond to Ransomware Attack

- **Implement Cybersecurity Response Plan**
 - **Call law enforcement (federal, state)**
 - **Call individual(s) trained to respond**
 - **Call consultants, lawyer, insurer**
 - **Assess what happened, damage**
 - **Use backup data (infected?)**
- **Communicate with clients, others**
- **Press release, website, social media**
- **Negotiate with attackers?**

Ransomware Resources

Virtual Practice

- **Cybersecurity & Infrastructure Security Agency**
- **CISA Website: Blog, news, links, “How do I . . .”**
- **Ransomware Guide: Two Parts**
- **Part 1: Ransomware Prevention Best Practices**
- **Part 2: Ransomware Checklist**

Remote Access Risks

Remote access to firm's computer system creates risks

- **Strong passwords can stop brute strength attacks**
- **Multi-factor authentication slows stolen password attacks**
- **Remote access risks may warrant hiring a consultant**
- **Safeguard servers, desktops, laptops, tablets**
- **Safeguard smart phones, copiers, scanners, IoT (lights)**
- **Staff changes: change user accounts, passwords – handout**

Password Fundamentals

- **Avoid weak passwords**
 - **can guess, e.g., password, 123456, 123456789**
- **8 or more characters**
- **Include CAPS, numbers, symbols**
- **Use leetspeak (or l33t\$p3ak)**
- **Consider pass phrases (5678 M@in \$treet)**
- **Use care with saving passwords**
 - **Not on post-it under mousepad**
 - **Not all in vulnerable document**

Mobile Devices

- Laptops, tablets, smart phones
- Have a PIN or stronger password (SIM swaps)
- Consider multi-factor authentication (awkward)
- Remote wiping
- Wiping after 10 failed password attempts
- Use Mobile Device Management
- Limit confidential information on device

Wi-Fi

- **WiFi “packet sniffing” – café or hotel hotspots**
- **Packet analyzer software available – e.g., Wireshark**
- **Without encryption, packets = plain text**
- **Microsoft exchange encrypts email**
- **“HTTPS:” in URL, encrypted email**
- **VPN connection secure, encrypted email**
- **Advise client; seek client consent**

Is Zoom (Videoconferencing) Secure?

Rep. Jim Jordan wanted Congressional Zoom meetings banned

- **Not end-to-end encryption; Chinese software, servers**
- **Meeting Zoom bombed? Only Waiting Room mistakes**

Zoom bombing: obscene images, racist messages

Free Zoom originally had no passwords, no Waiting Rooms

Zoom added those, working on improving encryption

Still safer than most cell phones, unencrypted email

Videoconferencing

Ala. Administrative Office of Courts – Apr. 8, 2020 Memo

- Courts use Zoom Professional, private setting, PIN required
- Third parties (e.g., Facebook) capture metadata – removed

Penn. Bar Formal Op. 2020-300 (Apr. 10, 2020)

- Working remotely, 14 pages – Rules 1.1, 1.6, 5.1, 5.3
- Provides 15 “Best Practices” – new, avoid Alexa
- Video conferencing – private, password, guard links

Computer Security – Misc.

- Wipe technology before discarding
- Investigate vendors (e.g., cloud)
- Consider data encryption
- Have employee termination process
- Separate work and personal computer use
- Regular backups (disaster recovery)
- Backup files in remote, unconnected place

Cybersecurity Insurance

Should you have cybersecurity insurance? Depends

Reduce loss risks, helpful audits, predictable expense

Tradeoffs:

- Expensive, not all losses covered
- Lose negotiation control, delay data return
- Limits, deductible can be discovered

Documents Hypothetical

- **Lawyer ships box of confidential documents as potential deposition exhibits**
- **Federal Express delivers box without some documents and with strange documents in the box, which has been re-taped**
- **Did lawyer fail to use reasonable efforts by using Federal Express to ship box?**

Documents Hypothetical (cont.)

- **Lawyer emails encrypted confidential documents as email attachment**
- **Lawyer emails encryption key (password) by separate email**
- **Did lawyer fail to use reasonable efforts by emailing encrypted documents and emailing password?**

PUBLIC WI-FI HYPOTHETICAL

Lawyer uses laptop in a coffee bar with public wireless internet access and uses WiFi to send and receive email with clients:

- **Are the communications privileged?**
- **Is the lawyer complying with her ethical duties?**
- **What should have lawyer done?**

PUBLIC WI-FI HYPOTHETICAL (cont.)

Depends: As to hypothetical, Cal. Bar stated:

Committee believes that, due to the lack of security features provided in most public wireless access locations, **Attorney risks violating her duties of confidentiality and competence** in using the wireless connection at the coffee shop to work on Client's matter **unless she takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall. . . . (cont'd)**

PUBLIC WI-FI HYPOTHETICAL (cont.)

Depends: As to hypothetical, Cal. Bar stated:

. . . Depending on the sensitivity of the matter, Attorney may need to **avoid using the public wireless connection entirely or notify Client of possible risks attendant to her use of the public wireless connection**, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so.

While Working Remotely (conclusion)

What are lawyers' ethical duties while working remotely?

Competence (Model Rule 1.1)

Confidentiality (Model Rule 1.6)

Supervision (Model Rules 5.1 and 5.3)

Remote: same ethical duties, increased technology risks

How manage those risks? Listened, see handout

大成 DENTONS

SIROTE

Thank you

J.S. “Chris” Christie

+1 205 930 5751

chris.christie@dentons.com

Dentons is the world's largest law firm, connecting top-tier talent to the world's challenges and opportunities with 20,000 professionals including 12,000 lawyers, in more than 200 locations, in more than 80 countries. Dentons' polycentric and purpose-driven approach, commitment to inclusion and diversity, and award-winning client service challenge the status quo to advance client interests.

[dentons.com](https://www.dentons.com)