Email Marketing in 2025: Debunking Myths and Discussing the Increased Risks under Federal and State Laws

Shahin O. Rothermel
Partner | +1 202.344.4550 | sorothermel@Venable.com

Ari N. Rothman
Partner | +1 310.229.9909 | anrothman@Venable.com

Jasmine Vidaurri Martinez
Attorney | +1 202.344.4249 | jvmartinez@Venable.com

VENABLE LLP

Applicable Federal Law: CAN-SPAM Act

VENABLE LLP

CAN-SPAM Overview

Congress enacted the CAN-SPAM Act in 2003 to establish uniform national standards for email marketing.

The Act creates a comprehensive framework that eliminates inconsistent state regulations across jurisdictions.

The Act creates a comprehensive framework that provides clear guidelines for commercial email practices.

The Act specifically prohibits the transmission of emails containing materially false or misleading headers, deceptive subject lines, and misleading content about the message's purpose.

CAN-SPAM's narrow preemption clause preserves state statutes that specifically prohibit **material** falsity or deception in commercial email.

VENABLE LLP

Fact or Myth?

Companies Must Have Affirmative, Opt-in Consent to Send Marketing Emails.

VENABLE LLP

MYTH: CAN-SPAM's Regulation of Commercial Emails

- CAN-SPAM **regulates** commercial emails.
- CAN-SPAM **allows** direct marketing email messages to be sent to anyone, without permission, **until** the recipient explicitly requests that they stop (opt-out).
- It **does not** ban sending unsolicited commercial emails.

VENABLE LLP

Navigating the Line: Is the Email Commercial or Transactional?

Commercial email: Primary Purpose

- **Promotes** a commercial product or service.
- Includes website content operated for commercial purposes.

Transactional or Relationship email: Primary Purpose

- Facilitates, completes, or confirms a commercial transaction.
- Provides warranty, recall, safety, or security information related to a product or service.
- Notifies recipients of changes to Terms of Service.
- Notifies recipients of changes in consumer's standing, status, or account information regarding:
  - Product or service updates;
  - Delivery of goods or services;
  - Subscriptions, memberships, or accounts;
  - Loans or employment relationships; and
  - Benefit plans.

VENABLE LLP

Requirements for Commercial Emails

- **Header Information**: No false or misleading header information.
- **Subject Lines**: No deceptive subject lines.
- **Transparency**: Clearly indicate commercial nature of message.
  - Identify the message as an advertisement.
  - **Note**: "ADV" or "ADVERTISEMENT" is **not** required.
- **Opt-Out**: Include a clear and conspicuous opt-out method.
  - Must remain operational for a minimum of 30 days; and
  - Must honor the opt-out request in 10 business days.
- **Contact Details**: Include sender's valid physical postal address.
- **Consent**: Subsequent emails can be sent only if the recipient has given affirmative consent.

VENABLE LLP

Prohibited Email Practices Explained

Prohibited Practices:

- False or misleading header information.
- Deceptive subject lines.

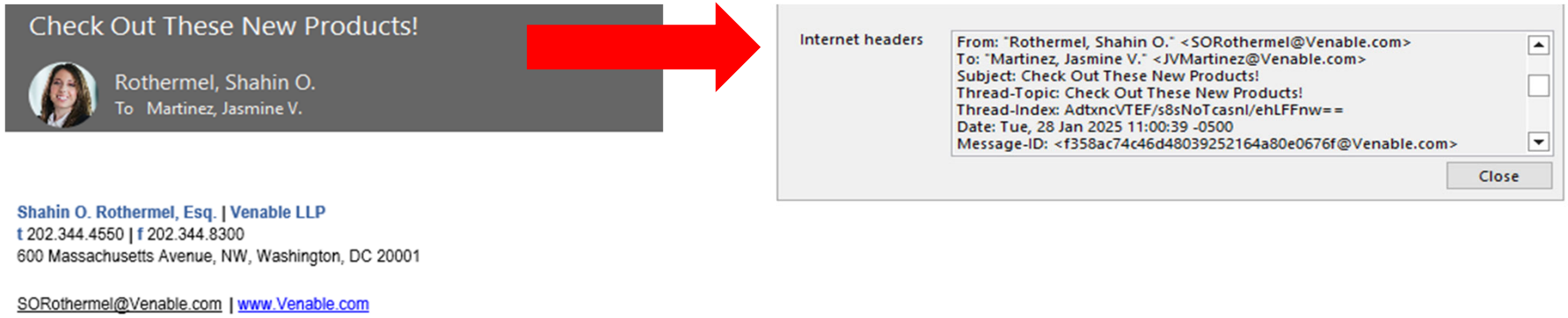
Commonly Challenged Email Practices:

- Unregistered domain names.
- False or proxy registered domain names.
- Misleading sender names or false identities in the “from” name.
- Name of a person/entity that is unavailable to response in the “from” name.
- Subject lines that would mislead a reasonable recipient about a material fact concerning the email’s contents or subject matter.
- Subject lines that imply a prior relationship if none exists.

VENABLE LLP

What Is Header Information?

- Header information includes the source, destination, and routing details of an email, such as:
  - Originating domain name;
  - Originating email address; and
  - Any information identifying the person initiating the message.



VENABLE LLP

Fact or Myth?

CAN-SPAM Does Not Provide a Private Right of Action.

VENABLE LLP

MYTH: CAN-SPAM Enforcement

- Generally **enforced by Federal Trade Commission** and state attorney generals.
  - **$53,088** statutory violation per email.
  - Criminal CAN-SPAM statute imposes criminal liability.
- **Limited** private right of action to Internet Access Services.
  - *Xmission v. Trimble*; *Xmission v. PureHealth Research*; *ZooBuh v. Savicom.*
- In an action by an Internet Access Service:
  - Up to **$100 per violation** of Section 7704(a)(1) of this title; or
  - Up to $25, in the case of any other violation of section 7704.
  - Damages can be trebled.

VENABLE LLP

Fact or Myth?

CAN-SPAM Preempts All State Email Marketing Laws.

VENABLE LLP

MYTH: CAN-SPAM's Preemption and Savings Clause

- The CAN-SPAM Act **preempts state laws**, but its **savings clause preserves state statutes** that specifically prohibit ***material*** falsity or deception in commercial email.
  - "Falsity" and "deception" maintain their ordinary meanings.
  - Deception requires ***more*** than minor errors.
- For a state law to survive, it must regulate ***material*** falsity or deception rather than technical violations or formatting issues.

Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348 (4th Cir. 2006).

- The Fourth Circuit found the claims preempted where the plaintiff alleged that the sending domain was not linked to the defendants because the challenged emails were "chock full of methods to 'identify, locate, or respond to' the sender or to 'investigate [an] alleged violation'" of the law.
- The emails contained a opt-out method, a link to the advertiser's website, and the mailing address and local phone number for the company.
- The Court explained, "If the alleged inaccuracies in a message containing so many valid identifiers could be described as "materially false or materially misleading," we find it hard to imagine an inaccuracy that would not qualify as "materially false or materially misleading."

VENABLE LLP

California's Anti-Spam Law

VENABLE LLP

Fact or Myth?

California's Email Marketing Law Does Not Provide a Private Right of Action.

VENABLE LLP

MYTH: California Anti-Spam Law Enforcement

- The California Anti-Spam Law **creates a private right of action** for recipients.
- Allows recipients to seek monetary redress.
- Applies to individuals or entities involved in commercial email advertising **sent from California or to California email addresses**.
- Holds **companies liable for actions of affiliates** and third-party email vendors.

VENABLE LLP

California: Prohibited Email Practices Explained

- Prohibits **unauthorized use of third-party domain names** in commercial emails.
- Prohibits sending commercial emails with **falsified, misrepresented, or forged header information**.
- Prohibits **misleading subject lines** that do not reflect the true content of the commercial email.

VENABLE LLP

California: Header Information Requirements

Falsified, Misrepresented, or Forged Header Information:

- Headers must be **truthful** and **non-misleading**.
- Must **accurately convey source**, destination, and routing information:
  - Originating domain name email address; and
  - "From" line or "from" name.

What Makes a Header Materially False or Misleading?

- Changes that obscure the sender's identification;
- Concealment preventing service providers from processing emails; and
- Changes that hinder the recipient from contacting the sender.

VENABLE LLP

California: “From” Name Requirements

- **D/b/a Name Requirements**:
  - Proper registration; and
  - Accurately identifies sender (person/company).
- **Acceptable identifiers**:
  - Legal company name;
  - Brand names;
  - Trade names; and
  - Business division names.
- **Best Practices**:
  - “From” name should match the sending or advertising entity.
- **Caution**: Even if registered, liability risks exist if it is too generic.

VENABLE LLP

California: "From" Name Cases

Rosolowski v. Guthy-Renker LLC, 230 Cal. App. 4th 1403 (2014).

- **Holding**: The court held that even if the "from" names were not the sender's official name and the domain name was untraceable via a WHOIS search, the plaintiffs could not establish a claim under Section 17529.5(a)(2) where the sender's identity was readily ascertainable from the email body.
- The court reasoned that the plaintiffs could not plausibly allege that the sender attempted to conceal its identity, as the sender's purpose of the email was to market his website, which was linked in the body of the email encouraging the recipient to make a purchase.

Silverstein v. Keynetics Inc., No. 16-cv-00684, 2016 WL 7475616 (N.D. Cal. 2016).

- **Holding**: The court dismissed the "from" name claims alleging they were "fictitious and false," and "misrepresented" the sender in an attempt "to trick the recipient into opening the email," because the plaintiff fails to allege that the email headers were materially false or deceptive and were therefore preempted by the CAN-SPAM Act.
- Here, the plaintiff did not allege that the individuals named in the "from names" were *actually* known to him; that the email senders misappropriated or "spoofed" their identities; or that the "from" names deceived him about the nature of the email.
- The court found that the "from" names "relate[d] to, at most, non-deceptive statements or omissions and a heightened content or labeling requirement."

VENABLE LLP

California: "From" Name Cases (cont.)

Greenberg v. Digital Media Sols., LLC, 65 Cal. App. 5th 909 (2021).

- **Holding**: The court held that the recipients failed to state a cause of action under Section 17529.5(a)(2) based on the allegations that the "from" names consisted of generic phrases like "Vehicle Service Plan" or "Vehicle Protection Info."
- The court reasoned that as in *Kleffman*, such phrases make no representation regarding the email's source, either express or implied, within the common understanding of that term, so they cannot be said to constitute "misrepresented" information.
- Moreover, the court explained that as in *Kleffman*, "a contrary conclusion would raise significant preemption problems," given federal authority holding that the CAN-SPAM Act preempts "a state law requiring an e-mail's 'from' field to include the name of the person or entity who actually sent the e-mail or who hired the sender."

VENABLE LLP

California: Domain Name Requirements

Registration and Use

- Must use exclusively owned domain names.
- **Prohibited practices**:
  - Using third-party domains without permission;
  - Creating variations of third-party domains, such as:
    - "123BankofAmerica456.com"; and
  - Providing inaccurate registration information.
- Plaintiffs allege that domains must be openly registered.

Technical Requirements

- Must be aware of routing through third parties, such as:
  - AWS;
  - IMGUR; and
  - GOOGLE.
- Must maintain:
  - Contracts showing permission;
  - Documentation of routing agreements; and
  - SPF records for authorized servers.

VENABLE LLP

California: Domain Name Cases

Kleffman v. Vonage Holdings Corp., 49 Cal. 4th 334 (2010).

- **Holding**: The California Supreme Court held that an email with a generic, nonsensical domain name that is accurate and traceable is not "misrepresented" header information because it makes no *affirmative* representation or statement of fact that is false, even if the sender chose the domain name for the purpose of bypassing spam filters.
- The Court explained that the use of an accurate and traceable domain name in an email cannot reasonably be understood to be an implied assertion that the source of that email is different from the source of another email containing a different domain name.
- Moreover, the header information in each of the 11 emails contained the term "GreatCallRates" in the part of the sender's email address that preceded the domain name.
- **Note**: Here, the defendant was the advertiser and was being sued for its marketing agents sending 11 unsolicited email advertisements. None of the domain names provided any indication to the recipient (or its spam filter) that the advertisement was from the advertiser, Vonage.

Balsam v. Trancos, Inc., 203 Cal. App. 4th 1083 (2012), *as modified on denial of reh'g* (Mar. 21, 2012).

- **Holding**: The court held that the header information was deceptive and constituted a falsification or misrepresentation of the sender's identity because the commercial emailer *intentionally* used privately registered domain names in its headers that neither disclosed the true sender's identity on their face nor permitted the recipient to readily identify the sender.
- The court explained that unlike in *Kleffman*, the sender's "salient motivation" was not to bypass spam filters, rather to prevent recipients from identifying the true source of the emails, or to contact the sender, but having no way of linking to the source.
- **Note:** Here, the defendant was not the advertiser but a third party that sent email on the advertiser's behalf, and it was sued for failing to identify itself sufficiently.

California: Domain Name Cases (cont.)

Wagner v. Spire Vision LLC, No. C 13-04952 WHA, 2015 WL 876514 (N.D. Cal. Feb. 27, 2015).

- **Holding**: The court granted summary judgment because the emails in question "provided a hyperlink to the advertiser's website, an unsubscribe link, and a mailing address for the sender…[consequently] [t]he sender's identity could thus be readily ascertained from the bodies of the emails."
- The court explained that what matters is whether the sender's identity is readily ascertainable from the body of the email.
- Here, the recipient provided no evidence that through the hyperlink to the sender's website, the active unsubscribe link, and the physical mailing address, the sender's identity could not be readily ascertained.

Greenberg v. Digital Media Sols., LLC, 65 Cal. App. 5th 909 (2021).

- **Holding**: The court found that an email with a made-up and untraceable domain name affirmatively and falsely represents the sender has no connection to the actual sender.
- The court explained that because the complaint here alleges that the domain names were essentially made up and untraceable, the materiality of such representations is not appropriate to resolve on demurrer.
- **Note**: Here, the defendant was the advertiser, and it was being sued for third-party senders' failure to identify themselves sufficiently.

VENABLE LLP

California: Subject Line Requirements

Content Guidelines

- Subject lines must accurately reflect the email's content.
- Evaluated in conjunction with the email body.
- **Must not** mislead about:
  - Email content;
  - Subject matter; or
  - Existing relationships.

Common Alleged Violations

- Implying existing relationships, such as:
  - "Congrats on your new personal record";
- Inappropriate use of "Re:";
- False urgency in promotional deadlines;
- Misleading advertising claims; or
- Incorrectly stating the duration of a promotion.

VENABLE LLP

California: Subject Line Cases

Rosolowski v. Guthy-Renker LLC, 230 Cal. App. 4th 1403 (2014).

- **Holding**: The court held that the subject lines were not likely to mislead a recipient acting reasonable under the circumstances, about a material fact regarding the content or subject matters of the email message because the e-mail advertisements made it clear that a free gift was conditional upon a purchase.
- The court explained that the subject lines' mention of a free gift clearly indicated that the gift was contingent upon making a purchase.
- The court found that the recipient's argument unpersuasive, as it turned on whether the emails' subject lines are misleading, not whether the email are misleading in their entirety.

Fact or Myth?

Private Plaintiffs Can Recover under California Law, Even if They Do Not Open the Email.

VENABLE LLP

FACT: Recipients Can Challenge Emails Even if They Do Not Open the Email

- In *Silverstein v. Keynetics*, the court explained that like the TCPA, Cal. Bus. & Prof. Code § 17529.5 "identifies a substantive right … that suffers **any time**" a prohibited spam message is transmitted. No. LACV1804100JAKAGRX, 2018 WL 5795776, at *9 (C.D. Cal. Nov. 5, 2018) (emphasis added).

VENABLE LLP

California: Penalties

- **Actual damages** for violations may be awarded.
- Damages up to **$1,000 per email** sent.
- Maximum liability "per incident" is **capped at $1 million**.
  - But what is an incident?

VENABLE LLP

Fact or Myth:

California's Email Marketing Law Is the Only One Companies Should Worry About.

VENABLE LLP

MYTH: Multiple Other States Regulate Email Marketing

- Washington's Commercial Email Marketing Act, RCW 19.190.020.
- Maryland's Anti-Spam Law, Md. Code Commercial Law § 14-3002.
- South Dakota's Anti-Spam Law, SDCL § 37-24-42.
- D.C.'s Commercial Email Marketing Act, D.C. Code § 28-5002.
- Georgia's Email Marketing Law, O.C.G.A. § 16-9-101.

VENABLE LLP

Washington Commercial Email Marketing Act: RCW 19.190.020

- The Washington State Legislature created CEMA "to address unwanted e-mail messages."
- Enacted in 1998, CEMA's false or misleading subject line provisions were included in the original statute.
- In 1999, the Washington Legislature amended the commercial e-mail provisions:
  - It clarified that assisting or initiating the transmission of a commercial e-mail violates the CPA.
  - It also declared that commercial e-mails containing false or misleading subject lines violate the CPA.

VENABLE LLP

CEMA Explained

- The law **prohibits** transmitting emails that:
  - Use a third party's internet domain without permission;
  - Misrepresent or obscure their point of origin;
  - Misrepresent or obscure transmission path information; and
  - Contain false or misleading subject lines.
- Applies to **any person** or entity sending commercial emails **from Washington or by a Washington resident**.
- Companies are **liable for actions of affiliates** and third-party email vendors.
- Recipients of unlawful commercial emails can pursue civil action under the CPA for: statutory damages and actual damages.
- **Damages to the Recipient** of an Email: Up to $500 per violation or actual damages—whichever is greater.
- **Damages to an Interactive Computer Service**: $1,000 or actual damages—whichever is greater.

VENABLE LLP

Washington: CEMA Cases

State v. Heckel, 122 Wash. App. 60 (2004).

Holding: The court affirmed the trial court's order granting summary judgment to the State where the spam clearly fell within the prohibitions contained in the Act: The spam was accompanied by misleading subject lines; was transmitted along misleading paths, and nine of the spam messages used the domain name of a third party who had not given permission to the defendant to use that inactive domain name.

- Here, the defendant did not deny that he violated RCW 19.190.020(1)(a) by using the domain name "13.com" without the permission of the name's owner.
- The defendant argued:
  - The State failed to present evidence that he sent any email to an email address that he knew or had reason to know was held by a Washington resident.
  - The court should consider the first line of the body of the email or the whole message of the email rather than viewing the subject line alone, however the court found this unpersuasive.
- Here, the subject line was clearly designed to entice the recipient to open the message, not with creative advertising as the defendant argues, but by enticing the recipient to believe that the message might be from someone he knows who is trying to "get the right email address" or who is sending something confidential, rather than a commercial advertisement.
- The court explained that CEMA addresses false and misleading information in the subject line, not in the body of the email, as the subject line serves to disclose the content of the email.

Washington: CEMA Cases

Gordon v. Virtumundo, 575 F.3d 1040 (9th Cir. 2009).

Holding: The Ninth Circuit held that the CEMA header information claims were preempted by CAN-SPAM because the header deficiencies relate to, at most, non-deceptive statements or omissions and a heightened content or labeling requirement and therefore affirmed summary judgement.

The plaintiff argued:

- The headers in the emails at issue—specifically, the "from" lines—violated CEMA because they failed to clearly identify the emails' sender and therefore misrepresented or obscured the identity of the sender.
- It was a violation of CEMA to require consumers to engage in an extra step to identify the sender, such as reviewing the message content or consulting a WHOIS-type database.
- CEMA requires that the sender or a client's name expressly appear in the "from lines."

- The court explained that because the claim involved "incomplete or less than comprehensive information" regarding the identity of the email sender, it did not amount to falsity or deception under the CAN-SPAM Act and were therefore preempted.
- Such technical allegations regarding the header information find no basis in traditional tort theories and therefore fall beyond the ambit of the exception language in the CAN–SPAM Act's express preemption clause.
- The court emphasized that assuming they are actionable under CEMA, they falter under the weight of federal preemption.

Federal CAN-SPAM Enforcement

VENABLE LLP

US v. Verkada Inc. (2024)

- The FTC, through the Department of Justice (DOJ), filed a complaint against Verkada.
- **Unlawful Conduct**:
  - Sent over 30 million unsolicited commercial emails over three years;
  - Failed to provide an unsubscribe option;
  - Ignored opt-out requests from recipients; and
  - Did not include a physical postal address in emails.
- **Proposed Order**:
  - Verkada must pay a record $2.95 million penalty for the CAN-SPAM violation.

VENABLE LLP

US v. Consumerinfo.Com, Inc. (2023)

- This case, filed in the U.S. District Court for the Central District of California, concerns Experian's unsolicited emails to users with free Experian accounts.
- **Unlawful Conduct**:
  - Emails lacked mandatory opt-out notices or mechanisms; and
  - Misleading content suggested they contained vital account information, despite being commercial in nature.
- **Proposed Order**:
  - The federal district court issued a stipulated order preventing Experian from sending commercial emails without opt-out notice and mechanism; and
  - Civil penalty of $650,000 for violating the CAN-SPAM Act.

VENABLE LLP

Ways to Reduce Risk

VENABLE LLP

Due Care Policy

- California law provides a **due care defense** for email marketers.
- Implementing an email marketing compliance policy can **reduce statutory damages**.
- If proved, a court **may lower the liquidated** damages to:
  - $100 maximum for each unsolicited commercial email advertisement; or
  - $100,000 maximum incident.

VENABLE LLP

Obtain Opt-In Consent

- California law only provides a private right of action for "unsolicited" commercial email advertisements.
- "Unsolicited" means:
  - The recipient has not provided direct consent to receive advertisements from the advertiser.
  - The recipient does not have a preexisting or current business relationship, as defined in subdivision (l), with the advertiser promoting the lease, sale, rental, gift offer, or other disposition of any property, goods, services, or extension of credit.

VENABLE LLP

Enter Affiliates with Strong Protections and Monitor Affiliates

Include Protections in Agreements:

- Representations and warranties;
- Limitations of liability; and
- Indemnification.

Monitor Affiliates' Activities:

- This will be a consideration in any due care defense.

VENABLE LLP