GORDON&REES
SCULLY MANSUKHANI
YOUR 50 STATE PARTNER™

E-Commerce Retailer
LEGAL GUIDE

Damon W.D. Wright
Gordon Rees Scully Mansukhani, LLP
Advertising & E-Commerce Group
PHONE: 703.973.8776
EMAIL: dwright@grsm.com

www.grsm.com

CONTENTS

ADVERTISING & E-COMMERCE GROUP

Damon W.D. Wright
dwright@grsm.com

Gregory Brescia
gbrescia@grsm.com

Clickwrap, Arbitration, and Class Waiver Now

DAMON W.D. WRIGHT · GREGORY BRESCIA

IMAGINE THAT RIGHT NOW, a litigious, opportunistic consumer is diligently searching the Internet. He goes from one e-commerce website to the next. At each, he doesn't stop to study the product images or features. He doesn't care about the product, the product claims, or the testimonials. But he knows what he wants to find. He keeps moving his mouse, clicking the hyperlinks, visiting the checkout page, and scrolling down the website terms. Halfway through the terms, he frowns. But he clicks away, goes to the next website, and keeps searching. He knows he'll find what he wants soon enough. And finally, he hits pay dirt. He has found an e-commerce website that does not have a clickwrap contract, a mandatory arbitration provision, or a class action waiver provision. He buys the most expensive product on the website and then takes a lunch break. He'll start working on his class action lawsuit in the afternoon. This fact pattern is fiction, but it could be real and it could be your website.

Many smart and driven e-commerce retailers spend countless hours sourcing their product and optimizing their website. This is very important of course. But somehow another very important, but extremely easy, part of building a successful brand too often goes overlooked. Including a clickwrap agreement on your checkout page and mandatory arbitration and class action waiver provisions in your website terms can literally save you millions of dollars.

A clickwrap contract is an online contract formed between a retailer and a consumer. But it isn't fancy. It is only a sentence next to an unchecked checkbox or above an "I Agree" button displayed in the body of the checkout page. And the sentence is simple—something like "I agree to the website terms of sale" or "By clicking 'I Agree' below, I agree to the website terms of sale" with the words "website terms of sale" hyperlinked to the complete terms. Where a consumer then affirmatively checks the unchecked checkbox or clicks the "I Agree" button and this is required before the consumer can complete a purchase, courts consistently find that the consumer is bound by and has agreed to the website terms of sale.

A browsewrap contract is very different, if it is a contract at all. A browsewrap contract is where the footer of a webpage contains the hyperlinked words "website terms of sale." Unlike a clickwrap contract, a consumer does not take affirmative action to agree and may not even see the hyperlinked words in the footer at all. Thus, courts typically hold that a browsewrap contract does not bind a consumer to anything. So while it is good to have the hyperlinked words "website terms of sale" in the footer, you should not rely on a browsewrap contract. You need to use a clickwrap contract to obtain the consumer's acceptance to the website terms.

Clickwrap, Arbitration, and Class Waiver Now

(CONTINUED)

This brings us to mandatory arbitration and class action waiver. The U.S. Supreme Court has held that mandatory arbitration and class action waiver provisions in website terms, where agreed to by the consumer, are enforceable to mandate arbitration and bar class actions, regardless of any state law to the contrary. This is one of the reasons it is so critical to use a clickwrap contract to obtain the consumer's acceptance to the website terms. You need the consumer's acceptance of the website terms to make the website terms, including mandatory arbitration and class action waiver provisions, enforceable against the consumer. Without acceptance, your website terms—even if brilliant—can be entirely useless. However, with acceptance and well-written mandatory arbitration and class action waiver provisions, you will have substantially insulated your business from any class action liability.

That said, this would only protect you from class action liability arising from sales on your website. It would not protect you from class action liability for products sold away from your website such as on Amazon or at a brick and mortar store. For these types of sales, and while the law is less settled here, you should include mandatory arbitration and class action waiver provisions in a packing insert placed inside your product retail boxes. This is known as a shrinkwrap agreement. It is important that the shrinkwrap agreement contain a notice that, by opening the box and then using the product, the consumer consents to the shrinkwrap agreement, including its mandatory arbitration and class action waiver provisions.

Now back to the hypothetical, but with a change. You've now worked with experienced counsel to make sure you have an enforceable clickwrap contract and enforceable website terms of sale, including mandatory arbitration and class action waiver provisions. The litigious, opportunistic consumer visits your website, is bummed by what he sees, and clicks away. The end.

Damon W.D. Wright
dwright@grsm.com

Craig Mariam
cmariam@grsm.com

Subscription Billing With Success

DAMON W.D. WRIGHT · CRAIG MARIAM

YOU SUBSCRIBE TO THOSE FTC ALERTS, but don't really read them. At most, you skim them for a split-second when they hit your email inbox. Over several weeks though, you realize that you seem to be skimming the exact same FTC alert every time. You think maybe the FTC is spamming you, sending the same FTC alert again and again. Going back and searching your past email, you then have a realization — "no, each of these FTC alerts is about a different FTC enforcement action, and the FTC keeps shutting down and taking millions of dollars from subscription retailers." You take a long pause because you're a subscription retailer. As you read more, you discover that in case after case the FTC is proving violations of something called "ROSCA." And businesses selling health and beauty products to golf balls to lingerie have been targeted and crushed. You immediately go to your website's check-out page and ask yourself "am I violating ROSCA?"

Getting Right With ROSCA

ROSCA is the acronym for the Restore Online Shoppers' Confidence Act, a federal law enforced by the FTC. ROSCA's focus is on preventing the situation where consumers purchase a good or service believing it is a one-time purchase without any further billing only to later have their credit card charged without consent. The FTC aggressively prosecutes subscription retailers who fail to comply with ROSCA, especially those who advertise a "trial offer." In those cases, the FTC often goes to court *ex parte*, i.e., without the defendants' appearance or even knowledge about the case, and obtains a court order freezing the business and the business owner's assets and appointing a receiver to take control of the business and the assets. This can have the practical effect of financially destroying a business and its owner before they know anything about the case or have an opportunity to defend themselves.

Although the consequences of violating ROSCA can be draconian, it is not hard to comply. ROSCA imposes requirements on e-commerce retailers who sell goods or services via a subscription billing or "negative option" plan. This is a billing plan where, after an initial payment, a consumer will continue to be charged and continue to receive a good or service indefinitely unless and until they take affirmative action to cancel. ROSCA has three requirements:

1. The retailer's website must provide consumers with clear and conspicuous disclosure of the subscription billing and cancellation terms;
2. The retailer must obtain a consumer's express, affirmative agreement to the subscription billing and cancellation terms before receiving a consumer's payment; and

Subscription Billing With Success
(CONTINUED)

3. The retailer must provide a simple and easy mechanism for a consumer to cancel.

What does this mean? For the first element, a retailer must disclose how much the consumer will pay during the subscription and how the consumer can cancel in plain English and conspicuous size font where a consumer is likely to see them. For the second element, a retailer should use an unchecked checkbox accompanied by the billing and cancellation terms, with the consumer required to check the checkbox and thus affirmatively agree to the terms before payment. For the third element, the retailer must let consumers cancel easily (e.g., by calling customer support, sending an email, or accessing their account online).

Thus, a retailer who buries the billing and cancellation terms in very fine print on the bottom of a check-out page has violated ROSCA. Likewise, a retailer who uses a pre-checked checkbox has violated ROSCA. And a retailer who makes it difficult for consumers to cancel, e.g., with a pattern of unanswered calls and long hold times when consumers call customer support or a protracted, stubborn effort to "save the sale" or "downsell" a consumer, has violated ROSCA.

To be sure, the FTC has made prosecuting subscription retailers who advertise a "free" trial and otherwise violate ROSCA an enforcement priority. However, the FTC has also prosecuted many subscription retailers who do not advertise a "free trial," did not intend to deceive anyone, and instead intended to comply and thought they complied with ROSCA. In some cases, the FTC has alleged that the billing and cancellation terms are too long or confusing, not in large enough font, or in an inconspicuous place on the website checkout page. In other cases, the FTC has alleged that text disclosing the terms above a "PURCHASE" or similar button, in lieu of an unchecked checkbox, does not constitute express, affirmative consent by a consumer. In other cases, the FTC has alleged that, although the initial checkout page may have complied with ROSCA, a retailer then violated ROSCA when using a "one-click upsell" to sell a second product on subscription without again clearly and conspicuously disclosing the terms or again obtaining the consumer's express, affirmative consent to the terms.

But Wait, The States Have Something To Say

In addition to ROSCA, many states including California, D.C., North Dakota, Vermont, and Virginia, regulate subscription billing. California has the California Automatic Renewal Law (Cal. Bus. & Prof. Code s 17600). This mirrors ROSCA, but adds two requirements. First, subscription retailers must send consumers a post-transaction email that reiterates the billing terms and how to cancel. Second, subscription retailers who take consumer transactions online must likewise provide the consumer with an online method to cancel, which may include email. California's district attorneys regularly prosecute subscription retailers for violation of the statute.

Many leading, brand-name subscription retailers have also been found liable in consumer class actions for violation of the California Automatic Renewal Laws and other similar state statutes. The consumer class actions often address what some would view to be minor technical statutory violations, for instance not disclosing how to cancel on the checkout page but instead having a "how to cancel" hyperlink that when clicked leads to a pop-up box. Like the billing terms (how much the consumer will pay), the cancellation terms (how the consumer can cancel) need

to be visible on the checkout page, without the consumer having to click anything to see them.

Visa and MasterCard Too

More recently, Visa and MasterCard have joined the effort to ensure consumers understand and agree to subscription billing and cancellation terms before purchase and are reminded about them after purchase.

In April 2019, MasterCard implemented rules mirroring ROSCA but adding requirements for post-transaction notification by subscription retailers to consumers about billing and cancellation terms. MasterCard's rules apply only to physical products and not digital products. MasterCard has instructed that subscription retailers who sell physical products must use MCC code 5968 (Direct Marketing—Continuity/Subscription Merchants) and TCC T (non-face-to-face) to identify all non-face-to-face negative option billing transactions and that these transactions and their merchants will be classified as high-risk.

In October 2019, Visa announced new rules taking effect in April 2020 that apply to subscription retailers who sell physical or digital products and offer a free trial or introductory offer that rolls into a subscription if not canceled. Along with mirroring ROSCA, the new Visa rules require post-transaction electronic notice to consumers about all billing terms as well as a link or other simple mechanism to cancel. The new Visa rules further require an electronic reminder notification with a link to online cancellation at least seven days before initiating a recurring transaction.

Visa and MasterCard have made clear that they are closely monitoring subscription retailers, especially those who advertise a "free trial." The card brands can also be expected to use mystery shopping to confirm compliance with their rules. Perhaps as much as the FTC, Visa and MasterCard have the power to end a business. Though card brand rules do not have the force of law, a subscription retailer who violates them could promptly be placed on the MATCH list and lose its credit card payment processing capabilities.

Your Next Steps

It may seem like subscription retailers are under attack. They should not be. Many time-strapped consumers count on household subscription goods and services to simplify life. One quick transaction and consumers can receive uninterrupted access to the latest streaming shows, months of lifestyle subscription boxes, or online cloud storage to back up all the family vacation photos. A subscription product and service can help improve people's lives. It is also not hard to comply with ROSCA and similar rules once you understand what you need to do.

But it is clear that regulators and the card brands have a negative view of subscription retailers who advertise a "free trial." It is also clear that, as aggressive action is taken against those who deceive consumers and disregard ROSCA, other subscription retailers will face scrutiny even if they have every intent to follow the law. A simple oversight like failing to disclose how to cancel on the checkout page can create liability and irreparable financial harm. To avoid this, your next steps should be to review your website's checkout page and post-transaction notification correspondence and to do so with experienced counsel.

Build Your Brand to Beat Infringers

SUSAN MEYER · BENNI AMATO · HAZEL PANGAN · DAMON W.D. WRIGHT

Susan Meyer
smeyer@grsm.com

Benni Amato
bamato@grsm.com

Hazel Pangan
hpangan@grsm.com

Damon W.D. Wright
dwright@grsm.com

THE NAME FOR YOUR HEALTH FOOD SUBSCRIPTION BOX came to you in a flash of genius late one night. Within months of product launch, sales were exploding. You thought about applying for trademark registration but figured that could wait because, right now, you're just focused on making money. Then one day, a friend mentions she saw your subscription box on-line at a much lower price than she thought you charged. Running a quick search, you discover a competitor has a product like yours with a name virtually identical to yours! Even worse, you then check out your BBB profile and see complaints from consumers who didn't even purchase from you but instead from the competitor! Realizing you need to take action fast, and wishing you'd done this earlier, you pick up the phone, call your lawyer, and ask "how do I stop this?"

You need to protect your brand. A brand is a company's lifeblood—it's how consumers recognize and identify your services and products over your competitors. Some of the world's biggest companies thrive on the strength of their trademark portfolio and consumers' recognition of the marks. Trademarks are like reputations—the stronger they are, the more well-received and credible the services and products offered under them will be. A strong mark translates into strong consumer recognition, and, in turn, strong sales and revenue.

Apply for Trademark Registration

A trademark is a source identifier: it lets consumers know a good or service is authentic. Trademarks don't have to be registered and are protectable under common law once a business uses a mark, as long as it is distinctive and the first to be used on that particular type of good or service. However, a business can also apply for a federally-registered trademark. This requires application to and approval by the U.S. Patent and Trademark Office ("USPTO"). If you are seeking to enforce your trademark against others, it is far better to have a federally-registered trademark than merely a common law trademark because a federally-registered trademark carries the presumption that you have priority over others across the country for that good or service.

Although the term "trademark" is sometimes used to refer to both types, there are two types of marks: trademarks and service marks. Trademarks are for goods, like shoes and athletic apparel by Nike®, high-fashion apparel and accessories by Chanel®, and computers by Dell®. Service marks are for services provided to consumers like fast food by KFC®, air travel by United®, and online search engine and advertising by Google®. But don't fret—you don't have to be famous to get a registration! The only requirements are actual use (sales of goods or rendering

the services to customers) across state lines or importing into the U.S. The U.S. even allows you to reserve a mark you intend to use through an "intent to use" application.

There are many benefits of registration. A registration provides public notice of the ownership of a mark and the legal presumption that the mark is owned by that business nationwide in connection with the goods/services listed in the registration. You have the ability to bring legal action against an infringer in federal court and to record the registration with customs authorities to prevent importation of infringing goods. Your mark is listed on the USPTO database, which is searched by third parties when looking at new marks, thus discouraging accidental infringement. You can also use your U.S. registration as a basis for registration in other countries.

Selecting a good mark is important because the USPTO will not register generic marks, like "beer" or "sweatshirt," and will not register merely descriptive marks, like "Beer House" or "California Sweatshirt," without showing the public recognizes that mark as yours already. You should also ensure that the mark you're thinking of using is not already being used by someone else for the same or a similar type of goods or services.

Before the registration is issued, a business should always use the ™ indicator to show that you claim rights to the mark. Once the mark is registered, you should consistently use the registration symbol ®.

Enforce Your Rights in Your Mark

You've worked very hard to create and build your brand, so it's very important that you take steps to protect your mark and take action against those who infringe upon it. Failure to take steps to stop the use of a similar mark in commerce potentially weakens your mark, risking the loss of the substantial goodwill that you've built in your mark, not to mention all of the hard work and money you've invested in promoting and advertising your brand, and developing and selling top-quality services and/or products under it.

Failing to protect your mark against infringing uses and allowing them to coexist can be deemed acceptance of those uses and diminishes your ability to challenge infringing uses. Plus, consumers who buy knockoff services or products under a copycat mark with the mistaken impression that they are buying your products could have a negative impact on your brand. Think about those misdirected negative reviews!

So, what exactly do you need to do?

First, after conducting a proper trademark search and selecting your mark, you should apply to register your mark as soon as you intend to use or begin using it in commerce. You should then, implement a program to monitor the use of your mark in the marketplace. This means checking the internet for potential infringing uses by conducting a Google search and searching social media. Next, you should sign up for a trademark watch service which monitor thousands of new federal trademark applications published by the USPTO in the *Official Gazette* each month. The service will alert you when another party applies to register the same or a similar mark in the same class of services of goods as your mark. You can then file an opposition to stop the registration of the other party's mark.

If you need to litigate to protect your trademark rights, you must prove protectable rights in a mark (a valid trademark registration is *prima facie* evidence of this, and conversely, failure to enforce your rights against infringers weakens the validity of your mark) and that the infringer's use creates a likelihood of confusion to the consuming public about the origin of the infringer's goods or services. Likelihood of confusion is measured by eight factors:

- the similarity in the overall impression created by the two marks (including the marks' look, phonetic similarities, and underlying meanings)
- the similarities of the goods and services involved (including an examination of the marketing channels for the goods)
- the strength of the trademark owner's mark
- any evidence of actual confusion by consumers
- the intent of the infringer in adopting its mark
- the physical proximity of the goods in the retail marketplace
- the degree of care likely to be exercised by the consumer; and
- the likelihood of expansion of the product lines.

The available remedies for trademark infringement include lost profits, disgorgement of the infringer's profits, injunctive relief, as well as potentially attorney's fees. If you prevail in a claim for counterfeiting, where the standard is essentially whether the infringing product and use of the mark are "nearly identical" to the trademark owner's product and use of the mark, you can recover between $1,000 to $200,000 in statutory damages per counterfeit mark, per type of goods or services sold, as well as potentially treble damages and attorney's fees or up to $2,000,000 if the counterfeiting was willful.

Use UDRP Proceedings To Seize Infringing Domain Names

If an infringer is using your trademark as part of their domain name, you can also take swift action to stop this. The Internet Corporation for Assigned Names and Numbers ("ICANN"), the organization responsible for coordinating and maintaining standards and procedures for domain name registration, instituted the Uniform Domain-Name Dispute-Resolution Policy (referred to as the "UDRP") to resolve disputes regarding domain names. While trademark owners can still request that a court transfer of a domain name as part of a lawsuit, UDRP arbitrations can effectuate a transfer cheaper and faster—usually within two or three months.

There are several arbitration organizations that handle UDRP arbitrations, but the two most widely used for U.S. trademark owners are the National Arbitration Forum (the "Forum") and the World Intellectual Property Organization ("WIPO"); their filing fees start at $1,300 and $1,500, respectively.

A UDRP complaint must provide facts and legal argument supporting the following:

- That complainant owns the trademark at issue;
- That the trademark was distinctive (or famous) at the time the domain name was registered;
- That the domain name is identical to or confusingly similar to (or dilutive of) the trademark; and
- That the registrant acted with a bad faith intent to profit from the mark.

While many registrants now keep their information private, the email addresses listed in the registry will still forward emails to the email address the registrant provided. Moreover, such privacy measures do not protect registrants from UDRP actions. Trademark owners can simply file the UDRP action against the domain name. The registrar will then be ordered to provide actual registration information, and the trademark owners will be given the opportunity to amend the complaint with this new information.

While UDRP actions may be faster and cheaper than litigation, they do have some limitations. An arbitrator can only determine who should own the domain name in dispute; they cannot stop the infringer from putting the infringing mark on the product packaging, nor can they stop the infringer from registering another confusingly similar domain name—at least, not until you file another action targeting the new domain name. UDRP actions also only apply to the domain name, so an arbitrator cannot adjudicate subdomain infringement or infringement anywhere other than in domain name. So if your infringer uses a subdomain like yourmark.nonfringingterm.net, or a webpage like www.noninfringingterm.net/yourmark, a UDRP action will not provide relief.

If Not Done, Apply for Trademark Registration Now

Returning to our hypothetical, our subscription box owner should have conducted a thorough trademark search and applied for registration before going to market. A registration may have deterred the upstart competitor by itself. But it's not too late to take action. Working with experienced trademark counsel, our subscription box owner has now applied for registration, sent a powerful cease and desist letter to the competitor, and caused the competitor to stop infringing—appreciating that they had put all of their profits at risk. And with federal registration expected in a few months, our subscription box owner has now strengthened the brand, made the business more valuable, and set themselves up to attack and prevent any infringement in the future.

Richard Sybert
rsybert@grsm.com

Damon W.D. Wright
dwright@grsm.com

Protecting Your Copyright (Your Ads) From Copying

RICHARD SYBERT · DAMON W.D. WRIGHT

YOU'RE PROUD OF YOUR ADVERTISING AND YOUR WEBSITE. You've optimized and split-tested all of it. Consumers click on your ads. Consumers convert on your website. The words, the colors, the graphics, the product images—all of it—is perfect. But it's not just consumers who are admiring it. So are others who are looking to ride your coattails, take advantage of your hard work and creativity, and copy, i.e., infringe your creation. You begin seeing competitor advertising with the same or substantially similar photos and text. You being seeing competitor website funnels that do the same. You then realize that competitors have even copied your code. It's like you've trained hard for a marathon, you're now running it with determination and a sense of accomplishment, and someone else has lazily stepped out of the subway near the end and is about to cross the finish line in front of you. You're pissed.

You can fight back. You own the copyright in your creative work. As a copyright owner, this means you hold the exclusive right as the creator of a creative work to reproduce the work. Advertising is protected by copyright, just like any other work of authorship, be it a book, song, or drawing. If you want to go after your infringing competitor for ripping your advertising, website, or code, or just want to be fully prepared in case this ever happens, here is what you need to do now.

Apply For Copyright Registration

Copyright arises automatically, the moment you create a work of original authorship. The degree of originality does not need to be much. It doesn't even need to be very good. It just needs to be original. You can put © 2019 Acme Anvil Co. on your ads and your website without anyone's permission. That said, if you take pride in your original work and want to prevent others from infringing or go after them if they do, you should absolutely register with the U.S. Copyright Office. It is not expensive. The fee is only $55 and the one-page form is fairly easy to complete.

Perhaps the biggest reason to apply for copyright registration is because this is a prerequisite for suing in court. But beyond this, it is important to apply for copyright registration soon after publishing a work. This is because a timely registration is needed if you want to have all available remedies if you sue for infringement.

If you apply for copyright registration within three months of the work's publication or before the infringement occurs, you can elect to recover either actual damages or statutory damages of up to $150,000 per infringement, plus attorney's fees.

Protecting Your Copyright (Your Ads) From Copying
(CONTINUED)

By contrast, without a timely registration, statutory damages are not available and your only option is actual damages—typically, either lost profits, a reasonable royalty, or disgorgement of the infringer's profits which can be nominal and difficult to prove.

The bottom line is because statutory damages may be higher and require far less proof than actual damages, you should register your work with the U.S. Copyright Office and do this as quickly as possible after the work is published.

Pursue Infringers For Compensation

Copyright infringement is the use of works protected by copyright law without permission. In a copyright infringement case, it is not necessary for a copyright owner to prove that an alleged infringer made an exact or identical copy of the copyright owner's original work. Rather the test is whether the alleged infringer's work is "substantially similar" to the copyright owner's original work.

To be sure, this test is not always clear-cut, exact, or precise. Because there is an element of subjectivity and perception with the "substantial similarity" test, reasonable people can disagree as to whether or not a work is "substantially similar" to another. The courts will also consider how much of the copyright owner's original work has been copied—the less that has been copied, the less likely a court is to find copyright infringement and vice-versa. Finally, an alleged infringer may assert various defenses, such as parody or fair use (e.g., educational purposes), though in most instances these defenses are not successful.

When you encounter infringement, you should promptly demand that it cease and should often demand compensation. If you have a timely registration and the copying is "substantially similar," you are in strong position to demand compensation because the alleged infringer is exposed to either actual damages or statutory damages, as well as attorney's fees. Although courts have pushed back against certain litigation tactics by "copyright trolls," a copyright infringement case can be expensive for an alleged infringer because they may end up paying not only their own attorney's fees but ultimately also the plaintiff's.

Pursue Infringers With DMCA Takedowns

The Digital Millennium Copyright Act (DMCA) protects website owners and online service providers from copyright infringement liability based on third-party content. But this protection requires that the website owners and online service providers comply with the DMCA's "safe harbor" rules and take down infringing content upon receipt of a lawful DMCA takedown notice. Notably, a copyright owner does not have to have a copyright registration to send a DMCA takedown notice. For a copyright owner that is facing infringement on Facebook, YouTube, or a website, a DMCA takedown notice can be an efficient tool for effective relief.

Comply With DMCA "Safe Harbor" Rules Yourself

If others can post third-party content on your website, you are at risk of being sued for copyright infringement. To avoid this, you should comply with DMCA "safe harbor" rules yourself. Among other things, this requires that you designate an agent to receive DMCA notifications; have the agent's name, address, phone number, and email m on file with the U.S. Copyright Office and available on your website; promptly remove or block access to infringing materials after copyright

owners give appropriate notice; and have adopted and reasonably implemented a policy to block posting by repeat infringers in appropriate circumstances.

If Not Done, Apply for Copyright Registration Now

Returning to our hypothetical, the same week he learned of the copyright infringement, our business owner applied to register his advertising, website, and code. He paid an extra $800 fee for each of three applications for expedited processing so he would get the registration more quickly. The same week, he sent a properly-completed DMCA takedown notice to the competitor's web hosting company which caused the competitor's website to be taken down and sent another DMCA takedown notice to Facebook which caused the competitor's Facebook page to be taken down. He has since demanded that the competitor cease any further infringement and pay either $150,000 in statutory damages or disgorge all of its profits, whichever is higher, to settle the matter. This competitor has been stopped in its tracks. The message has also made its way to others in the industry—this is one business owner you don't want to infringe.

Damon W.D. Wright
dwright@grsm.com

Mark Ishman
mishman@grsm.com

Advertising To Generate Sales, Not Suits

DAMON W.D. WRIGHT · MARK ISHMAN

YOUR SUBSCRIPTION PRODUCT IS AMAZING and you want the world to know. You also see competitors selling similar products and making outrageous claims about the product benefits. You know these claims are false, but also persuasive which is frustrating. Thinking about it, you decide you want to make the boldest product claims you can but without running afoul of advertising law—knowing this should be the best way to ensure customer satisfaction, build a strong and trustworthy brand, and also avoid regulatory or consumer class action. You think, "I'm okay if my product claims go up to the line, but I don't want to cross it." But then you ask yourself, "where is that line?"

To protect consumers, the Federal Trade Commission ("FTC") enacted the Federal Trade Commission Act ("FTC Act"), which empowers the FTC to investigate and prosecute businesses that engage in false and deceptive advertising practices that harm consumers. When the FTC brings an enforcement action against a business, the consequences can be severe and can include an asset freeze, disgorgement of all revenues, injunctive relief, and sometimes personal liability for the business owners. A business can also face attack for false or deceptive advertising from state attorneys general, local district attorneys, the Better Business Bureau, consumer class action counsel, and competitors, as well as consumer groups and the media. But before you become too frightened, please know that you can advertise aggressively and creatively and still comply with advertising law.

Have Substantiation for Your Product Claims

Under the law, claims in advertisements must be truthful, cannot be deceptive or unfair, and must be evidence-based. Thus, one of the most basic advertising rules is simply that, when you make a claim about your product, you must have substantiation to prove it. Here are some examples of common product claims and the type of substantiation you should have.

PRODUCT CLAIM	STRONG PROOF OF CLAIM
"Product Certified by Doctor"	A certification by a licensed doctor in the relevant field that your product works as advertised and based on appropriate tests or evaluations
"I Lost 2 Inches in My Waistline in 4 Weeks"	A statement from your actual customer who actually lost 2 inches in her waistline as a result of using your product

PRODUCT CLAIM	STRONG PROOF OF CLAIM
Before and After Testimonial with Photo	A statement from your actual customer that these pictures were actually taken before and then after using your product and the difference arises from use of your product
"Made in the USA"	Documentation from product suppliers establishing that "all or virtually all" of the product is made from U.S. sources
"Tests prove that [brand name] does [X]"	Requires "competent and reliable scientific evidence" to support the claim, e.g., double-blind, placebo controlled clinical studies of the product by qualified experts using accepted methods

It is important that the substantiation for product claims be compiled before—and not *after*—making the product claim. Once compiled, you should maintain a file that contains substantiation for each of your product claims. If a regulator contacts you and seeks substantiation for your product claim, it does not look good to request additional time to respond since you should have already had the substantiation on file.

Have Prominent and Accurate Disclaimers

A common misconception is that an otherwise unsubstantiated product claim is okay if it is followed by a disclaimer. It is not. Courts have consistently found that a disclaimer is ineffective and will be disregarded if it contradicts or significantly limits the product claim. To be effective, a disclaimer must be clear and conspicuous, in close proximity to the product claim, and not change but rather explain the product claim. For instance, if using before and after weight loss photos to show how your product can help people but the featured weight loss results are not typical, you should include a prominent disclaimer near the photos explaining "These results are not typical and most consumers who use our product and also exercise regularly should expect to lose [XXX]." Here again, you must also have substantiation, i.e., reliable clinical data, for the product claim made in the disclaimer.

Avoid Testimonials At Odds With Substantiated Product Claims

Another common misconception is that, if a customer provides a testimonial that truthfully recounts their experience and belief, the testimonial can be used without any further concern. This is not correct. The testimonial is still part of the retailer's advertising. Testimonials and endorsements cannot be used to make a claim that the retailer itself cannot substantiate. As such, the retailer cannot introduce a product claim through a testimonial that the retailer could not otherwise make themselves.

For instance, if a customer said "I'm sure this tooth whitening product will make your teeth two shades whiter, just like it did for me," the retailer could not use the testimonial unless it had substantiation for the product claim that this was a typical result. Or, if a customer said "this detoxification tea product helped to improve my memory" (which would be a drug claim), the retailer could not use the testimonial unless it had clinical studies to support that the product can in fact help to improve memory.

The same rules apply with dietary supplements. A customer may truthfully believe that a product helped cure their disease. The retailer may believe its product can do the same for the others. But unless the product has received FDA approval as a drug, the retailer cannot make disease claims or otherwise claim that the product affects the structure or function of the body. So the retailer cannot use the "cure disease" testimonial regardless of the customer's truthful belief.

Use Social Influencers but Disclose Any Connection

In recent years, there has also been an explosion in the use of social influencers in advertising. This type of advertising can be highly effective, but is also highly scrutinized. The key here is that, if the social influencer (or, for that matter, anyone who provides an endorsement or testimonial) has some "material connection" to the retailer (for instance, receiving money, receiving free product, or being an employee of the retailer), this connection must be disclosed. There are at least two reasons for this rule.

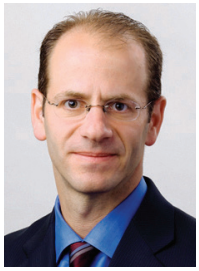
First, with social influencers' Instagram or other social media posts, the FTC wants consumers to understand when a post is in fact an advertisement. Second, because an influencer could be biased because of a material connection with a retailer (e.g., compensation), the FTC wants consumers to know when a connection exists so consumers can take this into account with their purchasing decisions. Words like "#ad, #sponsored, or #[brand name]ambassador" should be used or even something with a passionate tone like "I'm thrilled to be a brand ambassador for [brand name]." There can be room for creativity here.

Use Puffery

A final word about puffery. Puffery is advertising that makes exaggerated or boastful statements about a product that are not statements of purported fact, capable of being proven true or false, but rather are in the nature of subjective opinion. Puffery is allowed in advertising law, although the line between puffery and false advertising law can be thin and sometimes blurry. For instance, in selling a hair growth product, the statement "Women will love the way you look!" would be considered puffery, whereas the statement "Four out of five women will love the way you look" could be considered false advertising.

You Can Be Creative, Aggressive, and Legal

This is a very high-level summary of advertising law, and there are many complexities and finer points. Although not addressed here, the risks of violation can also be severe, including FTC and state attorney general action, consumer class action, and competitor lawsuits. And at the same time, a retailer that can smartly go up to the line, but not cross it, is in a strong position to build goodwill and customer loyalty. Many lawyers understand the law but not necessarily marketing. With experienced counsel who understands both, you can craft advertising that is creative, aggressive, and also legal.



Ronald A Giller
rgiller@grsm.com

Jennifer A. Guidea
jguidea@grsm.com

Compliance In Calling (And Texting) Customers

RONALD A GILLER · JENNIFER A. GUIDEA

YOUR NEW CBD ESSENTIAL OILS PRODUCT launched a month ago. You're getting hundreds of daily visitors to your website. But after filling out the name, address, and phone number fields, too many click away and don't convert. At a recent e-commerce mastermind event, a speaker tells you that, if you don't follow up with those visitors by phone and text, you're leaving money on the table. At a happy hour afterwards, another attendee approaches you and offers to sell you thousands of phone numbers for cheap—saying this is the easiest and fastest way to scale your business. This all sounds great, but then someone else mentions that their company did this, was sued for violating the "TCPA," and was hit with a seven-figure judgment. As they offer you a shot of bourbon, they say, "We could've done this the right way if we'd gotten good legal advice." You decide to buy the next round—and also get good legal advice.

While the business axiom "grow or die" has been widely accepted since George Ainsworth-Land's 1973 book by the same name, not all growth is equal. Often, the path to bigger is littered with landmines. Consider cold-calling. It has been around as a sales tactic likely since right after Alexander Bell connected his first telephone. Until fairly recently, the process was tedious, expensive and time-consuming. All of that has changed with the rapid explosion of new technologies. Suddenly, platforms and applications have become one-stop shops for generating lists of leads, efficiently calling or texting those leads and even allowing prospects to offer feedback electronically—all in a matter of minutes. While the potential for business development is virtually limitless, there are legal pitfalls that can undermine any benefits of such technology and negatively affect a company's bottom line.

The answer is that it depends largely upon how they are used. The Telephone Consumer Protection Act ("TCPA") and the Federal Communications Commission ("FCC") implementing regulations impose detailed restrictions upon the use of such technology. Congress, in enacting the TCPA, cited telephone privacy as the primary justification for the legislation. Despite years of enforcement and several FCC interpretive documents, the plaintiff's consumer bar is nothing if not creative, so there remain a number of grey areas where unsuspecting marketers might stumble into a violation. Before undertaking any marketing strategy involving cold-calling, text messaging or use of autodialing technology, businesses should take a hard look at the details of the campaign to ensure that any such risk is minimized.

So what exactly does the TCPA prohibit and require?

Don't Call Restricted Numbers

First, and perhaps most well-known, is the restriction on telemarketing calls to any person who has registered their telephone number on the national Do Not Call Registry. In addition to the national list, many states also have registries of numbers that do not wish to receive telemarketing calls. Moreover, the TCPA requires business and telemarketers to maintain records of called parties' requests not to receive future solicitations. Such requests must be honored for a ten-year period. A key component of this mandate is the requirement that telemarketers, whether within a business organization or hired as outside vendors, maintain written policies for developing and updating their do-no-call list and that all employees are trained to use the list. When faced with FCC inquiry or enforcement action (or the inevitable lawsuit), the policies and lists should be readily available for review.

Obtain Prior Express Consent

Similarly, business or telemarketers can avoid TCPA liability based on violation of do-not-call registries by keeping meticulous records of customers' prior express consent to be contacted via telephone and/or text. The TCPA permits telephone calls to subscribers who have given express written consent to be contracted by the specific caller. Consent must be evidenced by a signed, written agreement, whether in printed or electronic format, which states that the consumer agrees to be contacted by this seller and includes the telephone number to which the calls may be placed. Even if there is a continuing business relationship between the caller and the customer, if the customer has asked to be placed on the do-not-call list, the caller must honor that request unless and until the customer gives written consent to start receiving telemarketing calls.

Don't Call After Hours

Keeping with its genesis in the protection of consumer privacy, the TCPA also prohibits telemarketers from calling residential telephone subscribers before 8 a.m. or after 9 p.m. Similarly, the use of prerecorded or artificial voice messages calls to residences are prohibited. But what constitutes a "residential subscriber"? How does the TCPA deal with those individuals who choose to use their cellular telephone as their primary telephone to the exclusion of a traditional landline? While the FTC has not issued guidance on this point, several courts around the country have held that cellular telephone numbers are considered "residential" if the subscriber uses the number primarily for personal communications that are not associated with a business or commercial purpose. If in doubt as to how a telephone number should be categorized, the better practice is follow the proscriptions on calls to residential lines.

Use Human Intervention

Cellular telephones present other unique issues for the purposes of the TCPA. While the legislation restricts calls using automatic telephone dialing systems or artificial or prerecorded voices to cellular phones, there is still a great deal of confusion as to what that prohibition actually means. The TCPA defines "automatic telephone dialing system" as "equipment which has the capacity (1) to store or produce telephone numbers to be called using a random or sequential number generator, and (2) to dial such numbers. The FCC regulations add the requirement that such tasks must be accomplished "without human intervention."

Based on the language of the statute, and the subsequent interpretations by the FCC and the courts, it is clear that "predictive dialing" systems are prohibited. These platforms use a complex set of algorithms to automatically dial telephone number in a manner that "predicts" the time when a consumer will answer the phone and a telemarketer will be free to take the call. On the other end of the spectrum are platforms where users upload a pre-screened list of telephone numbers that are then automatically dialed by the technology. There are a host of variations in between and just as many inconsistent rulings by courts throughout the country. Given the confusion among consumers, telemarketers and the courts, the FCC has invited comments on the definition of "automatic telephone dialing system"—specifically the amount and nature of the human intervention required of such technology. No final report or recommendation has been issued, but various courts have stayed TCPA litigation pending clarification of the definition. If there is any doubt as to whether a platform or technology constitutes an automatic dialing system, counsel should be consulted to investigate how the term is defined in the specific jurisdiction at issue.

Assume For Now That Texts Are Like Calls

Yet another difficulty with TCPA compliance is that neither the statute nor the FCC regulations specifically address text messaging. Text messages have become a vital communication method that was virtually non-existent when the legislation was passed. For several years, litigants and the courts alike assumed that the same prohibitions that applied to calls to cellular telephones also applied to text messages. However, over the past several months, courts have called this interpretation into question, finding that text messages do not implicate the same privacy concerns as calls made to a residence or cellular telephone. One court has gone so far as to hold that receipt of a single text message is not sufficient to establish a TCPA violation as, without some aggravating factor, it does not constitute an injury or harm to the recipient. Despite this recent trend, caution should be used before embarking on a full-scale text messaging campaign given the unsettled state of the law. Again, counsel can assist with assessing the rapidly changing legal landscape.

Have Good Counsel For TCPA Compliance And, If Needed, Defense

If a telemarketer or business missteps and violates the TCPA, the consequences can be financially devastating. The statute provides for two separate private rights of action for aggrieved consumers. First, recipients of calls from automatic dialing systems or artificial or prerecorded voice messages may sue in state or federal court. Additionally, a consumer may file suit if he or she has received more than one telephone call within any 12-month period by or on behalf of the same company in violation of the do-not-call list prohibitions.

Each violation is subject to a $500 penalty, which may be trebled for a "knowing violation" of the statute. Courts are split on the specific definition of "knowing," but it appears the majority rule is that knowledge of the call itself—not necessarily that it constitutes a TCPA violation—is sufficient. Although $1,500 in damages likely won't break the bank, if a cold calling campaign reaches 20,000 consumers—a volume that is possible with today's technology—the potential liability increases exponentially and can have a real effect on even the largest company's bottom line.

Compliance In Calling (And Texting) Customers

(CONTINUED)

Navigating the TCPA involves avoiding many pitfalls in a rapidly changing climate. The law in this area continues to evolve and businesses may face significant risk of non-compliance even if they have the best of intentions. One of the best tools for those who conduct telemarketing or text campaigns is the involvement of legal counsel who is familiar with the current state of the law and of the emerging trends.

Damon W.D. Wright
dwright@grsm.com

Andrew Castricone
acastricone@grsm.com

Education On E-Mail

DAMON W.D. WRIGHT · ANDREW CASTRICONE

YOUR LEADING COMPETITOR IS DRIVING TRAFFIC to its website through email. You see that your competitor's email uses some unique abbreviations in the "from" and "subject" lines. You want to dive into email marketing too, but you've heard it is highly regulated. At a trade show, you also heard some folks complaining about how they had to pay a greedy plaintiff's lawyer $50,000 to settle a "17529" case. You think that had something to do with email, but aren't sure. You also know you don't want to pay any lawyer any money unless they're working for you. And with that last thought, you decide to talk to a lawyer.

There are both federal and state laws that regulate emails to consumers. The laws are intended to stop unwanted and deceptive emails, including by requiring disclosure of the actual source of the email. The good news is that compliance can be easy. The bad news is that penalties for non-compliance can be severe.

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act 15 U.S.C. §§ 7701-7713)

The CAN-SPAM Act applies to emails from your business where the primary purpose is commercial content or advertising. To a lesser extent, the CAN-SPAM Act also applies to emails relating to a transaction or a relationship with an existing customer if the email contains advertising. In all events, the email must not be false or misleading.

Although it has a criminal sounding name, this federal law may be enforced in a criminal, regulatory, or civil action. It also is not so much about pornography, but rather about "spam" email. Among its requirements, the CAN-SPAM Act prohibits sending commercial email to a recipient with: (1) false or misleading header information, (2) false or misleading contact information, or (3) deceptive subject lines that mislead the recipient about the content of the email. The FTC has provided these pointers on how to comply with the CAN-SPAM Act:

- **Don't use false or misleading header information.** Your "From," "To," "Reply-To," and routing information—including the originating domain name and email address—must accurately identify the person or business who initiated the message.
- **Don't use deceptive subject lines.** The subject line must accurately reflect the message content.
- **Identify the message as an ad.** The law gives you a lot of leeway in how to do this, but you must clearly and conspicuously disclose that your message is an advertisement.
- **Tell recipients where you're located.** Your message must include your valid physical postal address. This can be your current street address, a post office box you've registered with the U.S. Postal Service, or a private mailbox you've

registered with a commercial mail receiving agency established under Postal Service regulations.

- **Tell recipients how to opt out of receiving future email from you.** Your message must clearly and conspicuously explain how the recipient can opt out from future email.
- **Honor opt-out requests promptly.** Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message. You must honor a recipient's opt-out request within 10 business days. You can't charge a fee, require the recipient to give you any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an Internet website as a condition for honoring an opt-out request. You can't sell or transfer their email addresses, even in the form of a mailing list, except that you may transfer the addresses to a company you've hired to help you comply with the CAN-SPAM Act.
- **Monitor what others are doing on your behalf.** Even if you hire another company to do your email marketing, you can't contract away your legal responsibility to comply with the law. The company whose product is promoted and the company that sends the message may be held legally responsible.

The CAN-SPAM Act's requirements apply whether the email originates from you or a third-party sending email on your behalf. The FTC investigates and enforces the CAN-SPAM Act, and a private right of action may be brought by an internet service provider (ISP). It is important to comply because each separate email that violates the Act can result in penalties of up to $42,530 per email. In a government enforcement action prosecuting aggravated violations, there is also the potential for imprisonment.

Restrictions on Unsolicited Commercial E-mail Advertisers (California Business & Professions Code §§ 17529-17529)

Like its federal counterpart, California's "anti-spam statute" restricts the ability to send commercial advertisements originating in California or which are sent to a California e-mail address. A commercial e-mail advertisement is unsolicited if the recipient has not provided direct consent or does not have a preexisting or current business relationship. Unlike the CAN-SPAM Act, the California statute can give rise to a private right of action by the recipient of the email against the sender.

The statute applies to any U.S.-based company that sends emails to California consumers. It contains three categories of unlawful spam email that give rise to liability for advertisers and senders of commercial emails:

- the use of a sending domain name without the permission of the owner of that domain name;
- the use of false, forged or misrepresented header information, which includes the From email address, From name, and IP address of sending mail server; and
- the use of a misleading subject line.

The statute generally allows individuals (not just ISPs) to sue for statutory damages of up to $1,000 per email. However, if you have established and implemented

Education On E-Mail
(CONTINUED)

well-documented procedures to prevent the sending of unlawful commercial email (e.g. "opt-out" and "unsubscribe" mechanisms that are clearly communicated and actually work), the court may limit damages to a maximum of $100 per email.

Because the penalties for violating the CAN-SPAM Act or §17529 can be severe, you should work with experienced counsel to be certain that your emails are lawful and to prepare and help implement written procedures to honor opt-out requests. The same is true if you have engaged an email marketing company to send emails on your behalf. You need to know exactly what they are sending and should "seed" your email list so you can see exactly what they are sending. Your agreement with the email marketing company should contain a representation and warranty that they will comply with the CAN-SPAM Act and §17529 and require that they indemnify you for any violations. You must also be confident that they have the financial means or insurance coverage to honor the indemnification requirement. While your competitors may be violating these laws and making money at the moment, you're smarter than them if you recognize that an ounce of prevention is worth a pound of cure.

Rich Green
rgreen@grsm.com

Jeff Bouchard
jbouchard@grsm.com

Putting Privacy In Its Place

RICH GREEN · JEFF BOUCHARD

YOUR NEW "YARNS OF THE MONTH" subscription club has taken off. No sooner had you set up your website and started some marketing campaigns than customers from up and down the East Coast started signing up. Now, you're thinking big. You want to take things to Europe and the U.S. West Coast. You recently found a potential partner to help you launch that expansion. After an exciting first meeting they're all buzz kill when they inform you that you'll need to be CCPA-ready before you can get started in California, and fully GDPR compliant before you begin selling into Europe. At first you're dismissive, after all, this all sounds like it's "just compliance stuff." Then your new business partner tells you about penalties of €20M and how Google was fined $57 million for breaching the GDPR! You realize that these fines are serious and you had better be too.

These laws are serious and complex. But with good counsel working with your business, you can get on top of it all. Here's the deal—

GDPR

The General Data Protection Regulation or "GDPR" went into effect on May 25, 2018 replacing Europe's Data Protection Directive from 1995. The GDPR provides individuals with certain rights and control over their personal data. Personal data is defined broadly under the GDPR to mean any information relating to an identified or identifiable natural person and includes things such as name and email address but also includes location data and online identifiers (such as an IP address). The GDPR applies to *any* company, whether located in the EU or outside its boundaries, if that company processes (i.e., collects, stores, uses, discloses, alters, etc.) the personal data of individuals in the EU.

The GDPR applies to companies in one of two ways. First, if they are "established" in the EU, meaning they have an office, branch, agent, etc., regardless of whether they process the data in the EU. Second, if a company is not established in the EU but offers goods or services to people who are in the EU *or* if they monitor the behavior of people in the EU (i.e., tracking online or profiling individuals). For companies that match either of those criteria, the specific GDPR obligations imposed will vary depending on whether the company is considered a "controller" or a "processor." Controllers are the companies who determine what to do with the personal data they receive, while processors are those who process personal data on behalf of controllers. Processors do not make decisions about why the data is being processed.

Under the GDPR, controllers must ensure:

- personal data is processed lawfully,
- adequate security measures are in place to protect the data, and
- rights of individuals are protected.

Those individual rights include providing certain notices to data subjects, correcting or amending the data if it is inaccurate, deleting it under certain circumstances and providing data subjects with a copy of their data. Controllers are also responsible for monitoring those processors with whom they share personal data, and binding them to written contracts that contain certain provisions prescribed by the GDPR.

Since the GDPR's enactment, supervisory authorities (the governing bodies in each EU member state responsible for enforcing the GDPR) have brought numerous enforcement actions. There are two different tiers of GDPR fines. The one that applies to a particular situation depends on the nature of the violation. The first tier can see financial penalties reach €10M or up to 2% of a company's gross annual global revenue. Under the second tier, those figures can reach €20 M or up to 4% of gross annual global revenue.

CCPA

Experts debate whether the enactment of the GDPR was the result or the start of a global ripple in new data security and privacy laws. Whatever the case, the United States was part of that global wave of new laws. The most noteworthy of these new GDPR-like laws is the California Consumer Privacy Act or "CCPA" set to go into effect on January 1, 2020.

The CCPA governs the use of the personal information of California residents. Personal information is defined broadly under the CCPA and includes name, postal address, email address, IP address, social security number, biometric information, geolocation data, and internet activity information (i.e., browsing history and search history). The law applies to all for-profit companies doing business in California if they hit one of three triggers based on volume of data collected or revenue. Like GDPR, the CCPA grants California residents certain rights including the right to know what's been collected about them and how it's been shared. Companies must provide notice of their data collection, use and disclosure to California residents at the time of collection and again if requested by the data subject.

The CCPA provides a number of exemptions for information already governed by the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act. Recent amendments to the CCPA also provide a one year exemption on personal information collected in the employment context or used in certain business-to-business contexts.

In terms of penalties and fines, statutory damages under the CCPA range from $100 to $750 per data subject per incident. Penalties can be awarded by either a regulator or as the result of a court ruling if a breach of unencrypted personal information occurs due to a company's failure to implement and maintain "reasonable" security practices. This is often referred to as the CCPA's private right of action.

Your Privacy Action Plan

Complying with the GDPR and CCPA, as well as the approximately 11 other new data security and privacy laws that have been proposed in the US recently, may seem daunting at first. While it's true that there are variations among these laws, by focusing on their common themes, a pattern of basic building blocks for compliance begins to emerge, including:

- adopting a written risk-based technical and administrative data protection program,
- telling your employees and customers what you're doing with the data you collect about them and why,
- giving your employees and customers some degree of access to and autonomy over that data,
- keeping a close eye on third parties (including vendors) with whom you share that data, and
- responding swiftly to, and being honest with those affected by, unauthorized use if it occurs.

The GDPR and CCPA are two of the recently enacted data privacy regulations receiving a lot of publicity, but from Canada's PIPEDA to New York's recently enacted SHIELD Act, global and local governments are taking data security and privacy seriously with obligations increasing and fines for non-compliance growing. Fear not, however, because close collaboration between counsel, technologists and business teams, and the use of the building blocks referenced above, can make for cost-effective and flexible compliance programs that adapt to the ever-changing data security and privacy law landscape.

Michael Marino
mmarino@grsm.com

Richard Fallago
rfallago@grsm.com

Take State Sales Tax Seriously

MICHAEL MARINO · RICHARD FALLAGO

YOUR FLOWER POWER SUBSCRIPTION CLUB BUSINESS is a Delaware limited liability company with its principal place of business in Massachusetts. Flower Power's website is hosted through servers in Massachusetts. Its annual gross receipts are approximately $15,000,000. Flower Power has no retail storefront, so all sales are online through its website. Flower Power's sole member, Joe Bud, considers Florida his residence but keeps an apartment in Massachusetts. One Flower Power employee, Mary Jane, lives in Arizona, but all other employees reside in Massachusetts.

Why do these facts matter? To impose a sales tax on an e-commerce retailer, the retailer must have "substantial nexus" with the taxing state. But what constitutes a "substantial nexus" has recently changed. In *Quill Corp. v. North Dakota* (1992), the U.S. Supreme Court held that "substantial nexus" was, in essence, synonymous with a physical presence in the state. Under this test, Flower Power would only be subject to sales tax in Massachusetts and possibly in Arizona because of Jane's presence. But this changed with *South Dakota v. Wayfair* (2018), where the Court upheld a so-called "economic nexus" statute. Now a state can impose sales tax on an e-commerce retailer if the number or amount of sales with that state's residents create an "economic nexus" with the state, as defined by that state's laws. Put differently, Flower Power must now pay sales tax in every state imposing sales tax where Flower Power has an "economic nexus."

This has created serious uncertainty and complexity for e-commerce retailers. For years, many states had sales tax statutes that, although ostensibly applying to e-commerce retailers, were rarely enforced. Those states are now enforcing them. Likewise, about 40 states that did not previously have sales tax statutes that applied to e-commerce retailers have now enacted them. The states have thresholds for when the sales tax obligation is triggered, with the thresholds based on the dollar amount of annual transactions and/or the number of annual transactions and ranging from $100,000 to $500,000, although at least one state (Kansas) now has no threshold. Meanwhile, Avalara, TaxJar, and other businesses that provide automated sales tax compliance (tracking, collection, and remittance) and integrate with an e-commerce retailer's checkout page and CRM platform are thriving.

The challenge for states is determining who owes but is not paying sales tax. While a state may not have clear visibility into who owes but is not paying, we can anticipate what is coming. A state could send questionnaires to e-commerce retailers to obtain information about revenue and transactions from the state's residents. A state could use advanced statistical analytics to extrapolate and predict an e-commerce retailer's revenue and transactions from the state's

Take State Sales Tax Seriously

(CONTINUED)

residents. Further, a state could estimate a sales tax obligation by relying on data from e-commerce retailers who pay sales tax and have comparable size or market share to similar retailers who have not paid.

The states are rapidly galvanizing their sales tax collection and enforcement efforts. So the time is now, if not months ago, for e-commerce retailers to address their sales tax obligations. The failure to pay sales tax if owed can expose retailers to back taxes, interest, and penalties. In some states, a limited liability company's members may also face personal liability. If not yet done, an e-commerce retailer should promptly consult with a professional tax advisor and a sales tax compliance business so it can now collect sales tax from its customers and remit payment to states where sales tax is owed.

Richard Sybert
rsybert@grsm.com

Insuring You Are Insured

RICHARD SYBERT

FINALLY, YOUR E-COMMERCE GADGET BUSINESS is up and running. Initial operations funded, employees hired and trained, website up, money coming in, products going out. Time for just a little break. Hey, there's a football game on TV! But, man, what a lot of commercials... and what's with all these weird ads—geckos, emus, some naggy person named Florence? Wait a minute. They're all insurance ads. That's what we forgot. Don't we need insurance?

Yes, indeed you do. Running a business without insurance is as unthinkable as driving a car without car insurance, buying a home without title insurance, or raising a family without medical insurance. But exactly what kind of insurance does an online company, and specifically an e-commerce retailer, need?

Well, go full-on worst-case scenario for a moment, and imagine all the bad things that could happen to your business. A customer could eat or wear your product and contract a strange illness. An employee could get hurt on the job and sue. Bad guys could break into company premises and steal computer equipment. You could have a data breach, have your data stolen or compromised, and your customers' privacy rights violated (and guess who they're going to sue?). Your business could be interrupted by a fire, an ice storm, or an electrical outrage. Your competitors could steal your software or trade secrets, take issue with your advertising, accuse you of unfair competition. Let's face it, it's a jungle out there, with risks all around. That's why insurance got started in the first place.

This is no area for amateurs. You want to make sure your company is protected. So find a professional, licensed, established, and recommended insurance agent. A good agent, regardless of whether they work for just one insurance company or act as brokers representing many, will be able to assess your needs, obtain and compare quotes and coverages, and tailor coverage to your business. It makes the most sense to work with an agent or broker who has experience helping e-commerce retailers, so ask around (ask a knowledgeable lawyer) and get some recommendations, and interview more than just one. But at a minimum you will want to consider the following coverages:

Commercial General Liability (CGL)

This is the standard general business insurance and covers property loss and business liability, as well as other business-related risks (e.g., loss of income, employee theft, employee dishonesty, employees' personal property, and electronic data). Internet-based companies will want to ask specifically about "cyber" coverages. Make sure that you take the time to investigate the coverage limits and exclusions, and that you will be protected. You do not want to do this after a loss only to discover that there are gaps or exclusions in your coverage.

Particularly important is business interruption; if something happens and your business goes down, you want to make sure there will be enough money to recover and resume operations. And critical for all companies these days is data protection—not just insurance, but back-ups, redundant systems, and secure servers.

CGL policies should also provide coverage for any accidents, related defense costs, and judgments against the business owner and employees (see also EPL, below) from third parties such as customers.

Particularly important for Internet-based companies and others whose assets focus on intellectual property (IP) such as software, trade secrets, copyrights, trademarks, and patents is so-called "Advertising Injury" coverage. This differs significantly from insurer to insurer, so make sure you read each one carefully. A good Advertising Injury clause should cover claims against you for trademark and copyright infringement, false advertising, defamation, and trade secret misappropriation. The key is to include defense costs, because it can cost millions to defend one of these lawsuits.

If your brick-and-mortar facilities are located in a flood or earthquake zone, specific hazard insurance may be available (usually for physical losses only, not business interruption) as part of your general business insurance. Flood coverage is available from the federal government. Earthquake insurance is usually either an additional endorsement or a separate policy from a private insurer or, in California, from a state agency (the California Earthquake Authority, or CEA).

If you're selling products, whether online or not, you will also want to include product liability. For example, some box companies sell goods such as beauty products, and will want to be sure they get the correct coverage since many CGL policies exclude them (in which case, you may need a Professional Liability policy). An e-commerce retailer may want or need coverage for themselves as both a manufacturer and distributor; as a distributor, they may find their domestic liability exposure dramatically increased without solid contracts with foreign manufacturers.

Employment Practice Liability (EPL)

Employment practice liability insurance should provide coverage—although it may be limited—for claims from employees and former employees, such as alleged wrongful termination, discrimination, and sexual harassment. The employer who does not run into such claims is lucky. This should also provide coverage for vicarious liability in case an employee gets into an accident while on company business outside the premises.

Errors & Omissions (E&O)

This is basically insurance against lawsuits alleging professional negligence, or claims that your business's conduct fell below industry standards and caused harm or loss. Related to this is "D&O"—Directors and Officers, which is specifically directed towards claims (such as shareholder or investor suits) against officers and directors of the company.

Umbrella Coverage

An umbrella policy provides additional coverage above the usual commercial policy limits, in case of liability. Businesses are often attractive targets in a lawsuit, and an umbrella policy can offset that risk. Consider how much you would need to protect the value and operations of your business. Be absolutely sure the insurance contract spells out all coverage as well as non-coverage, and your own responsibilities as the insured.

Worker's Compensation

This is mandatory in nearly all states to protect your employees if they're injured on the job. Sometimes state agencies as well as private insurers will offer coverage. A certified public accountant can help navigate through the maze of local, state, and federal tax and employment regulations and be an invaluable resource—especially if you consult them early in the process.

Disability Insurance

A disability insurance policy covers a specific employee in the event that they cannot perform the work they want to perform. Most plans offer different options for waiting and benefit periods. For example, a plan may not pay until after 30, 60, or 90 days of disability. Benefit periods may last for 1 year, 3 years, 5 years, or up to age 65 years. Make sure the disability plan offers the ability to increase coverage limits each year, to grow with your business's success and growing revenues. Related to this is so-called "Key Man" (or "Key Person") insurance, which specifically insures against the loss or disability of mission-critical employees.

Life Insurance and Health Insurance

You might want to consider offering these benefits to your employees. As with the insurance industry in general, these products are heavily regulated to make sure they are not unfairly weighted in favor of owners and high-income employees, so you will want to consult closely not only with an insurance professional, but also with a legal specialist in these areas.

Now Relax

Many major insurers themselves offer helpful, easily accessible information online. For example, this page from Zurich Insurance, https://www.zurichna.com/en/prodsols, dives into the different types of insurance. An experienced lawyer can also help you engage with insurance professionals and review proposals so you get the right coverage, in the right amounts, and at the right premium. So now, if you've set the DVR on your television, skip the commercials and get back to watching that football game...

Advertising & E-Commerce Group

EXPERIENCE · ATTORNEY BIO

GORDON REES SCULLY MANSUKHANI

Advertising & E-Commerce Group

THE INTERNET HAS RADICALLY TRANSFORMED OUR ECONOMY, the way consumers buy and shop, and the way retailers capture their attention. Our Advertising and E-Commerce Group understands the unique business, legal, and regulatory issues that face e-commerce retailers, other online advertisers, and their service providers. The path from start-up to brand empire can be disrupted by many forces, including the FTC, state attorneys general, consumer class action counsel, online marketplaces, social media platforms, news media, traffic providers, payment processors, competitors, and counterfeiters. We proactively advise our clients on best practices to avoid these disruptions, and we effectively protect and defend our clients should these disruptions arise. We take pride in guiding our clients towards smart and sustainable growth.

OUR ADVERTISING AND E-COMMERCE GROUP PROVIDES LEGAL SERVICES IN THE FOLLOWING AREAS:

- Outside general counsel on advertising, regulatory compliance, intellectual property, contract, corporate, tax, employment, and other legal areas;
- Website funnel and advertising claims review for compliance with federal and state consumer protection laws, including the Restore Online Shoppers' Confidence Act (ROSCA), Section 5 of the FTC Act, FTC Endorsement and Testimonial Guides, FTC Business Opportunity Rule, and Cal. Bus. & Prof. Code §§ 17200 and 17500;
- Drafting website terms of sale, website privacy policies, intellectual property license agreements, and service provider agreements, including advertiser, affiliate network, fulfillment services, and social influencer agreements;
- Brand protection, including prosecution and defense in trademark infringement, UDRP domain transfer actions, copyright infringement, DMCA takedown notices, Lanham Act false advertising, product disparagement, and trade secret misappropriation litigation;
- Compliance, incident response, and management with the EU General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), as well as advice on email, SMS, and telemarketing laws;
- Avoiding and defending against consumer class actions, FTC and state attorney general civil investigative demands and enforcement actions, consumer complaints, right of publicity claims, and unfavorable news media coverage;
- Negotiating and litigating business disputes, including between retailers, lead generators, traffic providers, payment processors, and other service providers; and
- Strategic advice and counsel to improve customer experience, increase customer lifetime value, and strengthen business reputation and goodwill.

An e-commerce retailer who focuses only on aggressive advertising and short-term customer acquisition will not succeed. Nor will an e-commerce retailer who follows overly cautious and restrictive legal advice to avoid the slightest risk of potential liability.

With that in mind, we understand how to balance a client's passion for creative and evocative advertising with a client's desire for legal and regulatory compliance. The goals are not mutually exclusive and instead can coincide. Whether marketing health and beauty products, electronics, home furnishings, informational products, clothing, or coaching, our clients are driven, dynamic, and entrepreneurial. These qualities are maximized with effective counsel who knows the client's business issues, anticipates and protects them from legal and regulatory challenges, and cares about their success. This is what we do.

Representative Experience

- Represented company that designs and manufactures headphones in website privacy policies, trademark prosecution and defense, trademark infringement litigation, product disparagement, customs enforcement of trademark rights, brand protection, CCPA compliance.
- Represented technology company in hundreds of negotiations of customer contracts for subscription based software services.
- Represented technology company in multiple negotiations of contracts with partners and for the procurement of services, including cloud services and other technology based necessities.
- Defended online retailer in trademark infringement dispute involving costumes sourced from China.
- Defended computer consulting company in claims involving theft of trade secrets, copyright, and compute fraud and abuse claims
- Defended webhosting/design company in claims involving misappropriation of trade secrets and breach of contract.
- Represented large American clothing company in a class action unfair competition law complaint in San Diego.
- Completed numerous DMCA takedown notices on behalf of musicians and artists for infringing work.
- Represented food and beverage companies with respect to labels and advertising.
- Represented e-commerce retailer in defense of claims by purported brand owner with respect to trademark and copyright claims and unfair competition arising out of e-commerce website.
- Represented company related to Lanham Act and competitor claims on e-commerce site.
- Represented country's market leader for on-line submission of college admission applications as outside general counsel on all advertising projects, data privacy regulations, vendor technology and general commercial e-commerce contracts, and not for profit corporate matters.
- Former state securities regulator, federal prosecutor, and in house counsel at federal law enforcement agency responsible for overseeing or representing government agencies in state and federal enforcement actions such as seizures of websites marketing counterfeit products and securities fraud lawsuits as well as leading government agency efforts in state securities industry regulatory compliance and a variety of civil investigative demands.
- Former in house anti-counterfeit counsel at company that designs and manufactures protective solutions for smartphones and tablets, responsible for the development and execution of an anti-counterfeiting initiative within brand protection department involving identification of Lanham Act violations, negotiating out of court settlements, and collaborating with outside counsel handling Lanham Act litigation.
- Outside general counsel, Subscription Trade Association

Alexandria, VA
Washington, D.C.

PHONE
703.973.8776

EMAIL
dwright@grsm.com

Damon W.D. Wright

PARTNER

Damon Wright is a Partner in the Washington, D.C. and Alexandria offices of Gordon & Rees and a member of the Advertising & E-Commerce, Intellectual Property, and Commercial Litigation practice groups. Mr. Wright serves as outside general counsel to dozens of businesses and entrepreneurs who sell products and services online, including e-commerce retailers, technology companies, lead generators, advertising agencies, and related service providers. For these and other clients, his goal is focused and simple—to protect and strengthen their business.

Mr. Wright primarily focuses on online advertising, regulatory compliance, intellectual property, business transactions, and consumer protection law, as well as resolving, prosecuting, and defending against legal action. At the same time, clients rely on Mr. Wright for strategic advice and counsel with any legal need. As a trusted advisor and zealous advocate, he has helped clients proactively avoid, overcome, or achieve success in all variety of challenges. These include FTC and state attorney general actions, business and contract disputes, consumer class actions, trademark and copyright infringement, false advertising, unfair competition, defamation, right of publicity, fraud, trade secret misappropriation, negative media coverage, and other high-stakes matters.

Over his more than twenty years of practice, Mr. Wright has earned a reputation as a leader in the online advertising community. He understands the internet, listens and relates to clients, and knows how to achieve business growth with legal compliance. Mr. Wright serves as co-head of the firm's Advertising & E-Commerce practice group and is outside general counsel to the Subscription Trade Association and Responsible Traffic Association.

Representative Experience

- For online information product retailer, obtained multiple consent judgments, including substantial damages and permanent injunctions following trademark and copyright infringement by competitors
- At trial, represented newspaper in trademark infringement case and obtained permanent injunction requiring that competing newspaper change its name
- Represented international online dating service in lawsuit by competitor; prevailed on motion to vacate default and obtained dismissal of competitor's false advertising, trademark infringement, and unfair completion claims, with award of attorney's fees and costs
- Represented online computer and television retailer in defense of FTC investigation, resulting in closed investigation and no enforcement action
- Represented business owners in defamation action against consumer complaint website, defeating motion to dismiss that asserted Section 230 Communications Decency Act (CDA) immunity from liability
- Represented online nutraceutical retailer in evidentiary hearing before Better Business Bureau (BBB), persuading BBB to restore client's BBB accreditation and A+ rating

Damon W.D. Wright
(CONTINUED)

- Won sanctions, summary judgment, and affirmance on appeal—with actual damages, treble damages, and attorneys' fees—in false advertising case against online sports memorabilia retailer
- For online information product retailer, obtained arbitration award for actual damages and attorney fees against a serial plaintiff consumer on counterclaim for breach of prior settlement agreement
- Represented telecom software company in breach of contract action by reseller, with court dismissing all non-contract claims and granting summary judgment on contract claim, finding reseller could recover no damages
- Obtained preliminary injunction after evidentiary hearing for online health and beauty product retailer in trademark infringement, trade dress infringement, and misappropriation case against competitor
- Won sanctions, summary judgment, and affirmance on appeal in trademark infringement, fraud, and breach of duty of loyalty case between competing government contractors
- Represented software company founders at trial, against publicly traded corporation in a securities fraud, stock conversion, and shareholder dispute, obtaining compensatory damages, punitive damages, and sanctions
- Represented several high-net-worth clients in fraud and accounting malpractice lawsuits against national accounting firm, obtaining evidence that led to partial summary judgment, favorable settlements, and federal criminal prosecution
- In several confidential matters on behalf of various web-based business clients negotiated with national media outlets to retract, narrow, or balance otherwise unfavorable media coverage

Admissions

- Virginia
- District of Columbia
- U.S. Supreme Court
- U.S. Court of Appeals for the Fourth Circuit
- U.S. Court of Appeals for the D.C. Circuit
- U.S. Court of Appeals for the Ninth Circuit
- U.S. District Court for the Eastern District of Virginia
- U.S. District Court for the Western District of Virginia
- U.S. District Court for the District of Columbia
- U.S. District Court for the District of Maryland
- U.S. District Court for the Northern District of Ohio
- U.S. District Court for the Eastern District of Texas
- U.S. District Court for the Southern District of Texas
- U.S. Bankruptcy Court for the Eastern District of Virginia
- U.S. Bankruptcy Court for the District of Columbia
- U.S. Bankruptcy Court for the District of Maryland
- U.S. Tax Court

Damon W.D. Wright
(CONTINUED)

Education

- J.D., George Mason University School of Law, 1996
- B.S., Political Science, *cum laude*, James Madison University, 1993

Clerkship

- Honorable Barry R. Poretz, U.S. Magistrate Judge
  U.S. District Court for the Eastern District of Virginia 1996-1997

Honors

- AV® Peer Review Rated by Martindale-Hubbell, 2007—Present
- Included in *Washington, DC Super Lawyers,* 2012—Present
- Recognized as a "Top Rated Lawyer," *American Lawyer* and Corporate Counsel's Washington DC & Baltimore's Legal Leaders, Intellectual Property, 2013
- Recognized in *Super Lawyers Business Edition,* Business Litigation; Washington, DC, 2013
- Named Just The Beginning Foundation Diversity Champion, 2008
- Recipient, Benjamin R. Civiletti Pro Bono Lawyer of the Year, 2007
- Named T. Brooke Howard Fellow;
  Alexandria, Virginia Office of the Public Defender, 1994

Memberships

- General Counsel, Subscription Trade Association
- General Counsel, Responsible Traffic Association
- General Counsel, Together We Bake
- Member, Federal Bar Association
- Member, American Bar Association
- Member, International Association of Defense Counsel
- Past president, officer, and board member,
  Northern Virginia Chapter of Federal Bar Association, 2007 - 2015
- Frequently writes and speaks on litigation and internet advertising law

Damon W.D. Wright
(CONTINUED)

Community Involvement

PRO BONO

Since 2002, has represented Freddie Woods, recently obtaining the reversal of his 1997 capital murder conviction and death sentence

Represents Together We Bake, a job-training and personal empowerment program based on a micro-baking business and founded by his wife that helps women in need of a second chance develop employment and life skills

PERSONAL ACTIVITIES

An avid music fan, leads a group of friends and clients to the annual South by Southwest music festival

Represents musical acts, including Rusty Maples and Dave Gutter, lead singer of the bands Paranoid Social Club, Rustic Overtones, and Armies

Manages and plays percussion in Noise In The Basement, a local cover band and three-time winner of Law Rocks—DC, an annual battle of the bands competition

Plays adult coed soccer throughout the year

Has a teenage daughter at the College of William & Mary and two teenage sons in Alexandria, Virginia public schools

GORDON&REES

SCULLY MANSUKHANI

YOUR 50 STATE PARTNER™

www.grsm.com