Guide to Content Compliance for Financial Brands

BrandVerity

Table of Contents

Content Compliance for Financial Brands

When marketing financial services, you're constantly awash in a sea of acronyms. From the FTC to the FCC, the CFPB to the FFIEC, the TCPA to the FCRA, your task is never straightforward. Whether you're marketing loans, banking service, credit cards, or something else, it can start to feel like you're always one small step away from disaster. Every word published—by you, by a partner, by an affiliate, even by a consumer—seems to open you up to some kind of risk.

But fear shouldn't hold back progress. And while the advent of digital and social marketing has opened up new areas of risk, it has also opened up new avenues for expansion, growth, and marketing innovation. Paid partnerships, third-party vendors, affiliates, and social media platforms can be your most vibrant sources of advertising, new revenue, and brand growth—if used correctly.

Content Compliance: What Are We Talking about?

For the purposes of this guide, when we talk about "content compliance," we're talking about the content that third-parties, partners, affiliates, and consumers produce about your brand and that content's compliance with your partnership agreements, terms of service, and branding, as well as with federal, state, and guild regulations and best practices.

How This Guide Can Help

This guide provides information about how to mitigate the risk of working with various types of partners in a world where transparency, fairness, and accuracy is of the utmost importance. It's one thing to make sure that the content produced by your own marketing department adheres to the guidelines set out by state and federal agencies; it's another to make sure that every piece of information produced about you and your financial products by third-party vendors does as well.

By providing resources and information about who's responsible for managing compliance, how and why partner and affiliate sites fall out of compliance—both on accident and intentionally—and best practices for running a compliance process, we hope to help brands take charge of their online marketing efforts, for both their reputation and their bottom line.

How and Why Are Sites Non-Compliant?

Ensuring content compliance is a task in mitigating risk. It's impossible to know everything that might be said about your brand on all of the nearly 1 billion sites on the internet. Fortunately, the regulatory agencies aren't quite asking you to do that. That said, an understanding of why sites fall out of compliance, how to find sites that may be out of compliance, and what the the barriers may be to finding non-compliant sites gives marketers more insight into how to create, manage, and maintain their programs.

Who Is Responsible for Regulatory Compliance?

Long story short: **the brand itself**. While other parties such as networks and agencies may assist with compliance processes or even be subject to shared responsibility in contract terms, they do not typically face direct responsibility. A variety of cases and regulations over the past few years make it clear that state and federal agencies will hold advertisers responsible for claims and actions made by their partners and affiliates.

- Under **UDAAP**, banks are responsible for the actions of any third-party vendors or advertisers.
- The **FFIEC** recommends having clear policies and monitoring for social media use.
- The **CFPB** and, by extension, the **FTC** require that companies verify that all marketing accurately reflect the terms and conditions of the services and are comprehensible to consumers.

These lawsuits are expensive: CFPB fines alone can run in the tens of millions of dollars, and that does not include any potential redress for consumers.

The intentionally vague language built into these laws allows regulatory bodies and the courts a great deal of latitude in their enforcement. In general, we suggest being relatively conservative in your compliance process and monitoring. More monitoring, more controls, and more records will protect you if a governmental agency comes knocking.

Types of Publisher Sites

So, what do these sites look like? Before detailing compliance concerns, we want to make sure we're clear about the types of websites that are relevant to compliance. In our experience, these generally fall into four types:

Tracking Link Affiliates

These sites send traffic over to advertisers' (brands) websites via some form of tracking link, and are then compensated in some way for the traffic (typically for a conversion such as a sign-up or purchase).

In many cases, these tracking links are provided by intermediaries such as affiliate networks. In other cases, affiliates may send traffic directly to the advertiser's site, or sub-affiliates may send traffic through an affiliate and then over to the advertiser's site.

Examples include:

- Bloggers
- Card comparison sites
- Review sites
- Coupon, deal, and discount sites

Lead Generators

These sites encourage visitors to fill out forms with their personal information, then sell that information to various advertisers. Most sites offer incentives such as free quotes to motivate visitors to enter their information.

Examples include:

- Mortgage rate sites
- Loan quote sites
- Insurance quote sites

> ### The Schumer Box
>
> Since 1989, credit card issuers have been required to outline the terms of their card offers in a consistent format. All card promotions and offers must include the following:
>
> - Annual Fee
> - APR for Purchases
> - Other APRs
> - Grace Period
> - Finance Calculation Method
> - Other Transaction Fees

Multi-Step Lead Generators

Some lead generators present a series of forms to the visitor, rather than just a single all-encompassing form. On many of these sites, the initial form is used to collect geographic information about the visitor (typically the zip code), and then target offers based on that input. Within this multi-step arrangement, the advertiser (brand) often won't be shown until the visitor fills out an initial form and qualifies for an offer.

Examples include:

- Mortgage rate sites
- Loan quote sites
- Insurance quote sites

Marketing Partners

These sites generally have a direct relationship with your brand, typically through some sort of co-branded offering. Because of that, they may have permissions to promote your co-branded offering on their own, potentially requiring review or monitoring.

Examples include:

- Partner credit cards
- Lead-sharing agreements

Types of Non-Compliance

From our perspective, there are two kinds of non-compliant content:

1. Content that is in violation of your brand's terms, agreements, or policies; and
2. Content that is in violation of federal or state regulations.

There is, of course, overlap between these two kinds of non-compliance. Often, a site that is out of compliance with your terms and policies is also out of compliance with federal or state regulations. This makes sense, as not all of these policies are strictly to protect brand image. Many of the policies are developed so the brand can adhere to regulatory compliance standards.

Consumer Finance Brands Held Responsible for Affiliates' Indiscretions

Legal precedent states that brands will be held responsible for the deceptive advertising practices of their affiliates and partners.[1]

What Does Non-Compliant Content Look Like?

Non-Compliant content takes on a variety of forms and almost all exist at the intersection between the two types of non-compliance listed above. Some of the most common that we see are:

Incorrect Offer Details

Strangely enough, inaccurate offer information is actually quite common—not only on affiliate sites, but on partner sites as well (such as partner credit cards). Incorrect offer details very much qualify as UDAAPs and are forbidden by FTC and CFPB regulations as well as any good contract terms.

Legally, offer details need to be accurate, such that most consumers receive the advertised rates, all claims about fees are true and can be substantiated, and all endorsements are real. Further, when it comes to partner credit card offers, the financial institution backing the card must comply with the advertised terms—agreed upon or not—making it in everyone's best interest that all parties be on the same page.

Examples include:

- Misquoted figures (e.g. rates, terms, etc.)
- Out of date offers
- Improperly categorized offers (e.g. incorrect "cash back" or "bad credit" labeling.

1 https://www.ftc.gov/news-events/press-releases/2009/08/ftc-settlement-bars-deceptive-online-marketing-tactics-payday

Online Lenders Seeing Increased Regulatory Scrutiny

This year has seen payday and other high-interest lenders come under increased scrutiny from a variety of regulatory bodies. In particular, the FTC has filed a case against Sequoia One, LLC and Gen X Marketing Group, LLC for violations of Section 5 of the FTC Act. The FTC alleges that these companies improperly sold payday loan application leads without appropriate disclaimers to consumers.

Simultaneously, the CFPB has turned its attention to payday lenders by releasing a press release, factsheet and outline of the proposals it is considering. One of these proposals would require lenders to take steps towards ensuring that borrowers can repay their loans. CFPB Monitor has a great overview of these proposals.

Prohibited Text & Trigger Terms

Many companies also have words or phrases that their affiliates and partners are prohibited from using. Some of this prohibited text has to do with regulations (such as the federal Truth in Lending Act or the Fair Credit Reporting Act) while others have to do with protecting brands from potential consumer lawsuits.

Examples include:

- "no credit check"
- "cash today"
- "credit checks are not run in order to receive a loan"

Additionally, some brands require disclosures to go into effect when sites use certain "trigger terms" like the amount or percentage of a down payment or an interest rate. Again, the presence of a trigger term without a disclosure may not be in violation of any regulations, but it opens up a brand to unnecessary risk.

Lack of Appropriate Disclosures

If there's one thing the FTC has been incredibly clear on, it's that appropriate disclosures—on your site, on affiliates' sites, on social media, and on partners' sites—are crucial. Any material connection between someone endorsing or advertising a product and that product's manufacturer must be disclosed. In general, it's best practice to make sure that consumers are no more than one click away from the appropriate disclosure.

The 2012 update to the FTC's .Com Disclosures Guidelines, made even more apparent that disclosures need to be "clear and conspicuous" and that they should not be "relegated to 'terms of use' and similar contractual agreements." Further, they must include all *relevant* information, even if it is not specified by the regulations. Unfortunately, many bloggers, affiliates, and even paid partner sites and media continue to avoid placing appropriate disclosures on their pages. From affiliate social media posts to paid advertorials, all material connections must be disclosed.

Off-Brand Sites & Content

One of the most important things for a brand is where their content appears. Just as great ad space is important in the real world, it's important in the digital world as well.

Many brands state in their partner agreements that their information should not appear on certain kinds of websites: most notably sites with adult content, but coupon and discount sites are another common theme. Increasingly, brands are finding their ads, copy, and images appearing on sites they didn't approve and that have off-brand messaging.

Social Media, Web Forums, and Consumer Reviews

In December 2013, the FFIEC released "Social Media: Consumer Compliance Risk Management Guidance," a guide to existing laws and regulations regarding financial institutions' relationship to social media channels. At the end of the day, the guidelines are common sense: financial institutions need to be particularly careful when it comes to using social media and all existing laws and regulations apply with regard to social media.

Per the FFIEC, "social media" includes:

- micro-blogging sites (e.g. Facebook and Twitter)
- forums, blogs, customer review sites (e.g. Yelp)
- photo and video sites (e.g. YouTube, Flickr)
- professional networking sites (e.g. LinkedIn)
- virtual worlds and social games (e.g. Second Life, FarmVille)

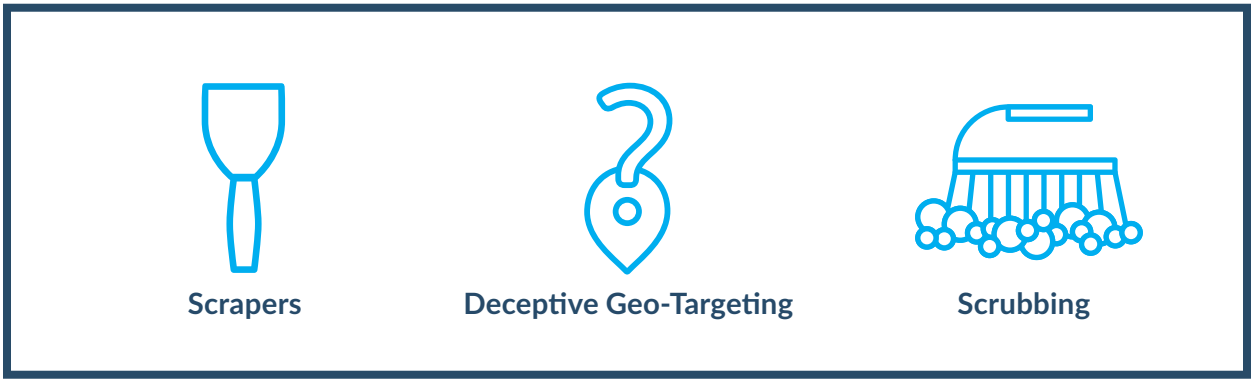
Employees should be adequately trained in how to use various networks and companies should have finely-tuned monitoring systems in place to know what is being said or shared about their company and its offers, as well as to respond to consumer complaints in a timely manner. Disclosures should be apparent in any post (or re-post) that serves as an advertisement. Working with consultants and agencies can sometimes heighten a brand's level of risk, so it needs to be monitored accordingly.

Degrees of Non-Compliance

While non-compliance comes in many forms, it doesn't always present the same severity. Broadly, there are three tiers of non-compliance:

1. Deliberately Malicious Activity
2. Misleading, Potentially Negligent Activity
3. Honest Mistakes

Tier 1: Deliberately Malicious Activity



Scrapers
While most non-compliant content appears on sites of known partners and affiliates, we are increasingly seeing brand-specific content appearing on sites that have no material connection with the company.

What do we mean by that? Scraper sites copy content from legitimate websites and re-post it on their own sites. The main reason to do this is (ironically) to seem more legitimate. Review or comparison sites will scrape high quality content from other places on the internet in order to appear to both consumers and search engines—which scan for the quality of content— to be higher quality than they are. We also see some tabloid news sites, paid media outlets, and bloggers and affiliates doing the same thing.

These sites can cause tremendous frustration and difficulty for several reasons:

1. **They don't make themselves known.** — These are not sites you're choosing to work with, and they are not going to inform you that they're stealing content from your or your marketing partners.
2. **Their content is never updated.** — These sites often pull old material in the first place, meaning whatever text, offers, or images they use are immediately outdated.

Further, because you have no connection to these sites, there is no way to get them updated.

3. **They may even outrank you.** — Because these sites scrape high-quality content from a variety of places, it is possible that they will outrank both you and your marketing partners in search. They also may run search ads or other types of advertisement to potentially divert your customers. This can cost you traffic and customers due to increased competition, friction, and confusion.

Telemarketing and Call Centers

Non-compliant phone calls from telemarketers and call centers are amongst the most common complaints in the CFPB's complaint database. And they can be non-compliant in a vast number of ways, from calling consumers without express written permission, to not revealing appropriate disclosures, to deceptive scripts regarding the purpose of the call. More information on the risks involved in using call centers and pay-per-call lead generators can be found on the BrandVerity Blog.

Deceptive Geo-Targeting

Many financial offers are location-specific. Mortgages, short term loans, and many other promotions are limited to certain states. They only apply to specific geographies or regions, so it is both deceptive and illegal to market these services outside of the approved locations.

Increasingly, we see offers being advertised in inappropriate markets—largely by affiliates who use sub-affiliate networks. This kind of action is, of course, both out of compliance with partnership agreements and with regulations. Unfortunately, however, it can be meaningfully profitable for a malicious partner to neglect these geographical restrictions. Tempting offers will still drive leads, and deceptive publishers are able to scrub their leads of any identifiers that might prove they were generated in a non-compliant manner. The result: financial brands pay for leads that were generated in bad faith, and that they can't actually sell to.

FTC Rules Advertiser Responsible for Fake News Sites Created by Affiliates

A federal court has sided with the FTC in a suit against LeanSpa, LLC and LeadClick Media that holds the advertisers responsible for the actions of their affiliate marketers and requires them to return $11.9 million to consumers. The court upheld the FTC's claim that LeadClick violated Section 5 of the FTC Act when its affiliates used "fake news sites" to promote products online. While LeadClick has maintained that they have no control over these actions, the court stated that "no reasonable jury could deny" that they "both participated in, and had the authority to control, the affiliate marketers conduct in so far as it related to the fake news sites." Both Performance Marketing Insider and Technology Law Source have written more in-depth analyses of this decision.

Scrubbing Information & Identifiers
Some publishers choose to scrub certain pieces of information (e.g. referring URLs, IP geolocations, addresses, etc.) from the leads they sell to brands. Of course, the removal of referrer IDs from leads does not necessarily mean that an affiliate, publisher, or partner is doing anything wrong. In fact, a fairly common practice to retain certain information so that they don't lose their competitive edge.

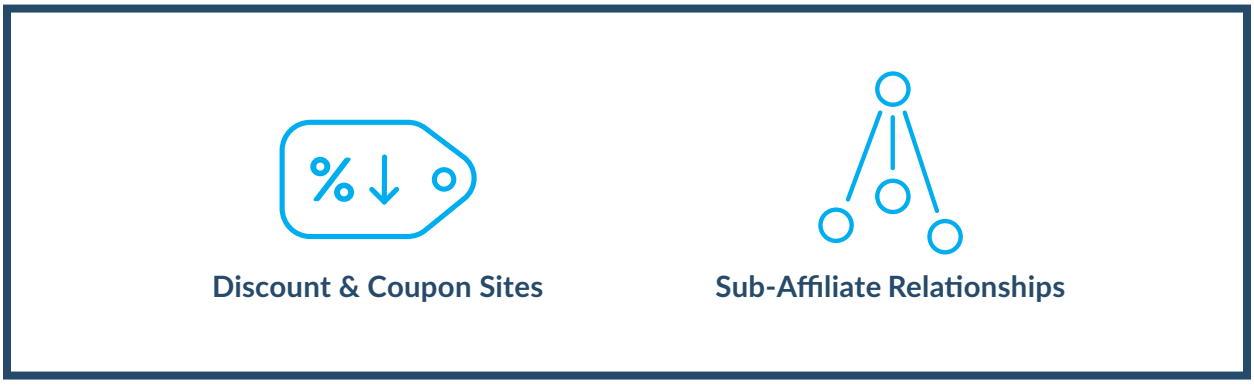
However, missing information can be a sign that your partners are trying to hide something from you. If you see an uptick in the number of leads coming in without referrer IDs, IP geolocations, or even zip codes, it's worth some additional examination. Ask your publishers what has changed and try to figure out what websites are driving those leads and how.

TPCA Disclosures

One of the most common missing elements on an affiliate or lead generation sites is a TCPA disclosure. This is especially relevant for mortgage brokers and other online lenders who collect telephone numbers and personal information from a variety of lead generation sources.

Contacting these leads is illegal and associated fines start at **$1500 per text message** sent and range from **$4,500 to $16k per phone call** made. When you account for the thousands of possible messages sent and calls made, those numbers add up very quickly. And, past precedent states that brands will be on the hook for these violations.

Tier 2: Misleading & Potentially Negligent Activity



Discount & Coupon Sites
Brands often find themselves appearing on coupon sites, which will offer deals like "$25 Bonus with New Checking Account" or "Earn 2x Rewards Points!" Many of these offers are copied from elsewhere around the web, expired, or simply nonexistent.

What's most interesting here is that most financial brands do not or cannot offer coupons at all. When you're providing financial products at market rates, there is no such thing as a coupon

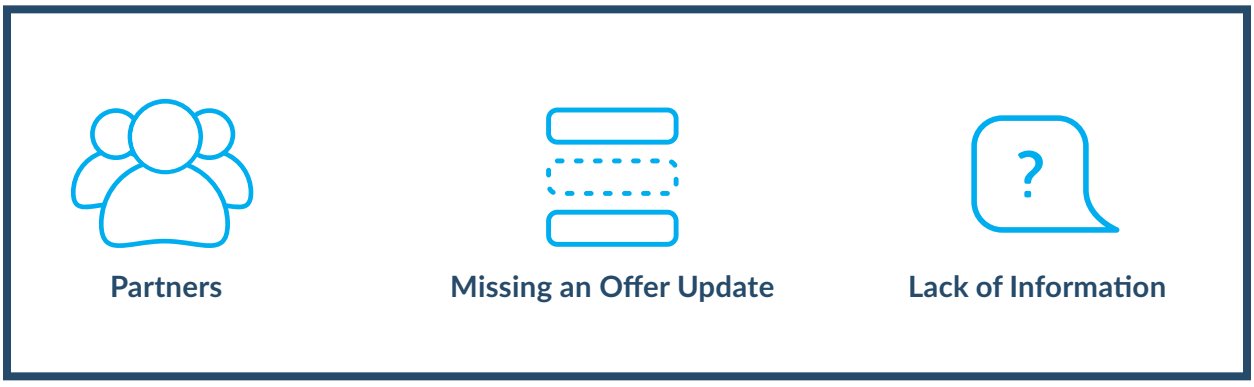
or discount. Other companies that purely connect financial brands with leads have no ability to sway things like interest rates. In either case, simply being mentioned on a coupon site may be misleading in its own right.

Sub-Affiliate Relationships
One of the main reasons that brands work with both affiliates and partners is to gain access to their traffic sources. But the nature of these traffic sources can open brands to increased risk. For example, many major affiliates have their own networks of sub-affiliates to whom they farm out business. Similarly, marketing partners may choose to work with affiliates (and therefore sub-affiliates) of their own.

These marketing partners do not always disclose who their sub-affiliates are. In fact, it's in their interest to keep that information secret. After all, if the brands knew who all those sub-affiliates were, they might choose to bypass the middleman and work directly with those publishers. This secrecy creates a couple of issues:

1. **Lack of Visibility** — You simply can't control what you don't see. When sub-affiliates are promoting your brand without your knowledge or oversight, that distance opens the door for a variety of compliance issues.
2. **Lack of Compliance Understanding** — It's very unlikely that these sub-affiliates are fully trained in regulatory compliance, meaning they are more likely to fall out of compliance than publishers that you work with directly. Although whatever party you work with directly should be accountable compliance within their network, it is far too easy for communication and responsibility to break down—particularly as the relationships become more diffuse.

Tier 3: Honest Mistakes



Some Partners Just Want to Do Things Differently
The most basic reason that sites slip out of compliance is fairly innocent: affiliates, partner sites (for example, partner credit cards), or paid media sites just want to do things a little differently.

They may change some copy, upload a new image, make an add-on offer that they think will better entice their readers.

For the most part, this kind of issue falls into that first category of content that violates your terms or agreements. Most programs and partnerships clearly delineate the official brand images and copy that should be used, and all should have strict rules around what kinds of offers can and can't be made. Partners and affiliates are expected to use that material and only that material for the offer itself.

That said, sometimes in changing an image or a piece of text, partners mistakenly put themselves in a state of non-compliance. While the materials you send over have already been cleared by your compliance team—moving a single word could change that.

Missing an Offer Update

One of the most common reasons for sites to become non-compliant is missing an offer update. Partners and affiliates face several challenges in keeping their content up-to-date with compliance demands:

- Large sets of pages to update (sometimes thousands),
- Short windows of time in which to update their sites for compliance, and
- Inconsistent timeframes and compliance requirements from different financial services companies.

Despite this complexity, any mismatch between a site's text and the actual terms of an offer can expose your brand to a variety of regulatory risks. Further, it creates the possibility for customer confusion—which is the very thing the FTC and CFPB most want to avoid.

While missing an offer update may not be malicious, per se, it is clearly in violation of a brand's partnership agreement and opens up the company to risk every time it happens. Also, some partners and affiliates may intentionally not change terms on time in order to try to drive more traffic with old, slightly more persuasive terms. This practice is dangerous for everyone involved, so partners who seem to consistently have trouble updating their pages should be removed from a program.

Lack of Compliance Knowledge or Information

Paid partnerships are a common way to build an online marketing presence. By partnering with another organization such as a review site, magazine, or news source, financial brands can place paid "advertorials" in places where potential customers are likely reading.

But these advertisements, although fully vetted through an in-house compliance team, can sometimes create unexpected risk when the partner organization is not as up to date on

compliance processes and procedures. Appropriate disclosures can sometimes disappear, or be printed too small to really see, and it can suddenly become very unclear that a material relationship exists between the two companies. When working with these kinds of paid partnerships, it's important to keep an eye on these pages to make sure they remain in compliance long-term.

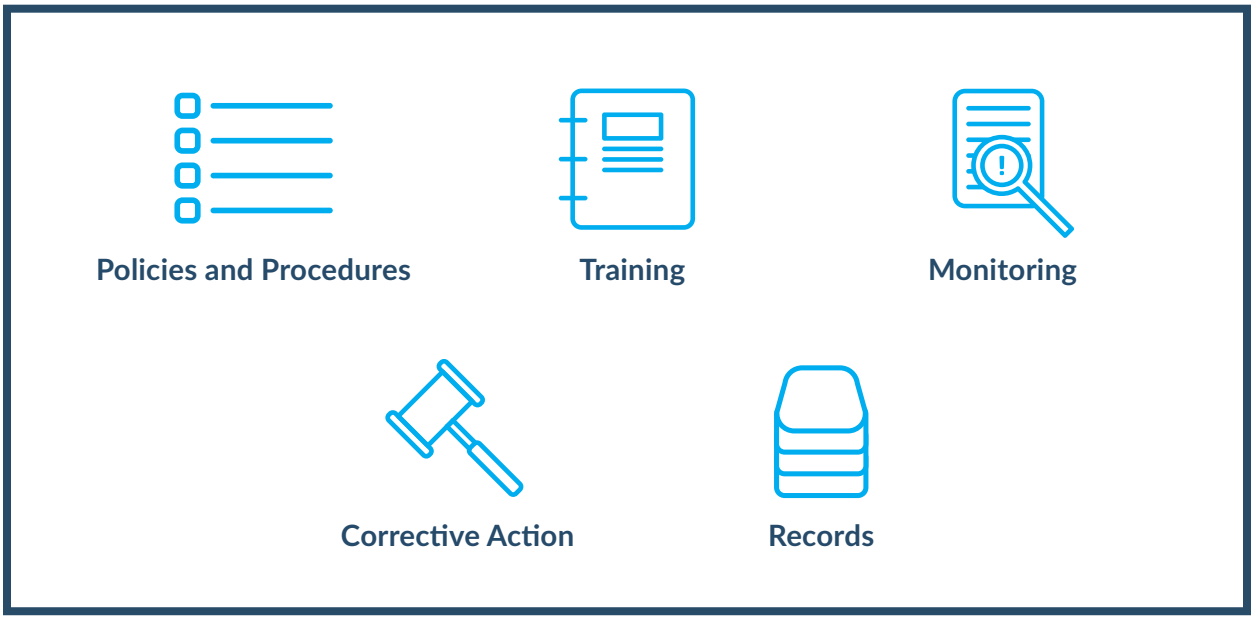
Mitigating Damage: Running a Content Compliance Process

An effective and efficient content compliance process can do a great deal to mitigate the inherent risk in working with partners and affiliates. Mitigating risk is the goal, of course. While these federal and state agencies will never exactly say this: none of them expect any corporation to know about, control, or read every single word written about them on the internet. It's simply impossible.

Organizations like the CFPB regularly examine and audit corporations to see if their processes are sufficient. Your process should be able to stand up to that scrutiny. What they expect is for there to be a clear, detailed process in place that can protect consumers in a reasonable way. They want advertising to be fair, transparent, and honest across all marketing channels.

These organizations do, however, remain vague about what, precisely, they consider reasonable. The following section will suggest some best practices for running a content compliance process based on interactions with our customers, lawyers, and other industry experts.

Components of a Content Compliance Process



A complete process for content compliance includes five parts:

1. Written policies and procedures
2. Training for your team and any partners who market your services
3. Monitoring (manual or technological)
4. Ability to take corrective action
5. Records that support the process

Written Policies and Procedures

The first step to an effective content compliance process is to have a set of written, transferable rules and regulations. Simply put, a process that relies on a single person is not effective. Someone needs to be able to read the written procedures and, from them, be able to both understand and enact the process.

Training

In addition to having a set of written procedures, it is key that all relevant members of your team, as well as your partners, understand not only that compliance is important, but what compliance really means.

Most important from a regulatory compliance standpoint is training of the company's Board of Directors, management, audit personnel, and staff in the rules and their responsibilities

regarding compliance, as well as in what processes the organization has in place. This kind of training is not optional in regulated industries. The CFPB writes in their Examination Guide:

> Board members should receive sufficient information to enable them to understand the entity's responsibilities and the commensurate resource requirements. Management and staff should receive specific, comprehensive training that reinforces and helps implement written policies and procedures.
>
> Requirements for compliance with Federal consumer financial laws, including prohibitions against unlawful discrimination and unfair, deceptive, and abusive acts and practices, should be incorporated into training for all relevant officers and employees, including audit personnel.

But, in addition to making sure your in-house directors, management, and staff understand both the importance and responsibilities of running a compliance program, it is helpful to engage your partners in this process as well. Often compliance programs will be, at least in part, implemented by third-party organizations such as affiliate networks, ad agencies, or marketing firms. Making sure these partners are fully-trained in UDAAPs as well as any specific-to-your-brand requirements will help ensure that nothing untoward slips through the cracks.

Running a Monitoring Process

The central, most crucial part of a content compliance program is the monitoring process. In most organizations, monitoring known sites is a highly scripted process. At regular intervals, a team of compliance professionals, each of whom is responsible for a subset of partner and affiliate sites, will conduct a full audit of known partner and affiliate sites.

How Often to Audit

Frequency of monitoring is often tied to changing offers for financial services. In general, publishers have between 24 and 72 hours (and sometimes only an hour or two!) from the time the brand informs them of a change to alter the copy on their websites. Once that time period is up, a compliance check usually occurs. This check, while focused on the specific changed text, should also scan for any other potential compliance issues (logos or other changed copy) at the same time. If offers are not being updated regularly, then compliance checks should be scheduled on a regular basis.

Steps to Take in an Audit

1. **Check Known Sites** — Most organizations keep track of known sites in a spreadsheet of URLs, usually ranked by importance to the brand, number of views, or revenue. Beginning with the top tier of sites, compliance managers go through each URL, checking the website for content compliance.

   In particular, they generally start by determining whether the site has changed since their last review. Based on the result, they may mark the site as compliant if no changes have been made, or conduct a full re-check if the content has changed. They will also click through each affiliate link to make sure it goes to the correct page and does not divert users improperly.

   This kind of manual checking requires vast amount of institutional knowledge as well as great attention to detail. Officers need to have clear knowledge about what can and cannot be said, what logos or images are allowed to be used, and which disclosures are necessary on each page.

2. **Mark Compliance Status** — Compliance officers will then return to the spreadsheet to mark the page compliant or non-compliant, as well as the time observed. Some companies will include notes, such as whether it was a category or product page. Additionally, some brands will assume that all category pages include the same content, and will not check beyond the first one viewed.

3. **Search for New Sites & URLs** — In addition to monitoring the sites listed on the spreadsheet, many companies also attempt to find new sites and pages that may have been added since the last review cycle. These sites and pages can be especially risky, not only because the brand previously had no visibility into them, but also because affiliates or partners may be obfuscating them intentionally.

   In some cases, monitoring these new sites is as easy as adding them to the spreadsheet once publishers have reported them to the advertiser. In others, it involves searching for specific brand names in Google and other search engines to discover previously unknown sites. If new sites are found, they are added to the spreadsheet and marked compliant or not.

4. **Contact Marketing Partners** — Once marked, if non-compliant, the officer will contact the partner or affiliate and record that interaction in the spreadsheet. Some companies, like they prioritize websites to review, will also prioritize issues about which to contact publishers. An out-of-date offer or improper disclosure, for example, might need to be addressed immediately, but out-of-order bullet points or slightly changed copy, might be addressed after the officer has completed his full review.

All of these interactions—viewing the sites, noting compliance, and contacting affiliates or partners—need to be time-stamped and saved, not only for the company's records but also in case any regulatory bodies conduct an audit. Those bodies will expect to see comprehensive, time-stamped records available for review.

Corrective Action

There are a variety of steps that can be taken if an audit discovers partners or affiliates out of compliance with either your agreements or regulations. Knowing what these steps are and how and when to enact them should be a key component to both the company's written processes and staff trainings.

- **The first step** is always to notify the site and allow the partner time to fix whatever has slipped, along with a firm warning. If it's an honest mistake, this should fully take care of the issue.
- **If you receive pushback** from a publisher, that could be a red flag. An honest partner should be happy to fix an issue and make sure they aren't opening you up to increased risk.
- **If you find scrapers** stealing your content or locate content on inappropriate sites, you should contact the website and attempt to have that information taken down. You may, depending on the type of content, also have a copyright claim. It may be worth having a legal team look into that possibility.
- And, **should you discover outright fraud** in your program—be it a repeated, small non-compliance or more egregious issues like improper geo-targeting—those partners should be reported to their superiors, payments cancelled, and they should be removed from your program. Allowing these kinds of behaviors to exist in your program only sends the message that you allow these kinds of marketing techniques, making your legal position less tenable, and opening yourself up to other issues.

Record Keeping

When it comes to regulations, it's always good to have a paper trail. While you could do this with literal paper, a digital set of records will probably be more reliable and easy to reference. In case of an investigation from a regulatory body, you want to be prepared with records that demonstrate a reasonably and repeatable process. While there isn't a clear set of requirements from any particular regulator, here are some general best practices to include:

- Documentation of what the typical process entails (whether it's daily, weekly, or monthly)
- Criteria of how compliance is evaluated in each case
- Records of each audit, including at least some examples of compliant content, non-compliant content, and content with possible compliance issues
- Documentation of all communication with affiliates and partners
- Documentation of affiliate and partner pages, including screenshots and the user pathway from the initial offer through to the final page they visited

Technological Solutions and BrandVerity

Until recently, few technological solutions existed to help corporations streamline and improve their content compliance process. Now, an increasing number of solutions exist that help brands create more efficient ways of monitoring the important, high-value sites they know about as well as discover the sites that slip through the cracks or are being intentionally hidden by deceptive advertisers. Technology like BrandVerity's suite of services helps brands improve their existing processes while also staying on top of new developments in content compliance so as to mitigate the damage that rogue partners can wreak on a marketing program.

If you're ready to update your manual process with some technology, BrandVerity's Content Monitoring can streamline your workflow and discover issues you may not even know exist. Contact us to talk to a sales representative and see how we can help you further reduce your risk level.

Resources

Key Terms in Regulation

Consumer Finance Protection Bureau (CFPB): The CFPB was established by Congress as part of the 2010 Dodd-Frank Act. Its goal is to eliminate unfair, deceptive, or abusive acts or practices (UDAAP) by financial institutions and to educate consumers about their relationships and agreements with financial corporations.

The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act): The Dodd-Frank Act was established to prevent another financial crisis like the one in 2008. It is intended to lower risk in the U.S. finance system. As part of its reforms, it established the CFPB to consolidate regulatory oversight from a variety of agencies under a single umbrella.

Unfair, Deceptive, or Abusive Acts or Practices (UDAAP): Defined by the Dodd-Frank Act, UDAAPs are misleading or harmful statements or behaviors made by those offering financial services or products to consumers. Rules regarding UDAAPs are made by the CFPB and enforced in part by the FTC.

Federal Trade Commission (FTC): The FTC is a federal agency tasked with both protecting consumers and ensuring strong competition in a variety of economic sectors. Among its many duties, it helps enforce the CFPB's regulations.

Federal Financial Institutions Examination Council (FFIEC): The FFIEC is an interagency body tasked with establishing uniform standards and reports for a variety of federal agencies that oversee financial institutions, including: the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB). Their 2013 Social Media Marketing Guidelines describe how financial corporations should interact with and monitor social media.

Fair Credit Reporting Act (FCRA): The FCRA primarily covers the use and dissemination of personal information by consumer reporting agencies. It does, however, also require those entities to make appropriate disclosures regarding cost and availability of credit reports and limits the ability of affiliates to sell information for purposes not adequately disclosed to the consumer.

Federal Communications Commission (FCC): The FCC is a Congressional agency that oversees and regulates communication by radio, television, wire, satellite, and cable in the United States.

Telephone Consumer Protection Act (TCPA): The TCPA is a federal statute administered by the FCC. Passed into law in 1991 and updated in 2012, the TCPA requires express, written consent for a specific seller to use an autodialer to call or text a consumer.

Financial Industry Regulatory Authority (FINRA): FINRA oversees broker-dealers in the US. It provides regulations and guidelines for advertising securities by both firms and professionals.

Useful Websites, Blogs and News Sources

Online Lenders Alliance (OLA): The OLA is an association of online lenders that sets industry standards and best practices.

FTC Beat: Published by Ifrah Law, this blog publishes regular updates and commentary about news in marketing regulation. The scope covers regulatory bodies beyond the FTC, including the FCC and others.

Davis Wright Tremaine: With practice expertise in Financial Services and Marketing, including an emphasis on regulatory compliance, Davis Wright Tremaine publishes advisory pieces and blog posts about regulatory news for financial brands.

Technology & Marketing Law Blog: Law professor Eric Goldman posts about topics from the FTC's .Com Disclosures to the use of trademarked terms as keywords in search engine advertising. Many of his posts are picked up by publications such as Forbes.

The Financial Brand: This site provides industry news with a focus on retail banks and credit unions. Articles range from topics such as best practices and insights to compliance and regulation.

American Bankers Association: This industry association aims to support banking institutions, large and small. Their website features an entire section devoted to compliance, and members have access to a special compliance library.

Risk & Compliance Journal: This division of the Wall Street Journal covers topics in corporate regulation, risk and compliance. Topics can range somewhat broadly, but often circle back to the finance industry.

CFPB Monitor: Published by Ballard Spahr LLP, this blog keeps a tight focus on everything CFPB-related, including regulatory updates, explanations, and guidance.

All About Advertising Law: Venable LLP runs this blog, which centers on regulatory topics such as the FTC and TCPA. The firm also regularly published industry articles and alerts.

Hinch Newman LLP: Attorney Richard Newman from Hinch Newman LLP blogs about legal compliance in the marketing industry.

Davis & Gilbert LLP: This firm provides regular alerts about case law related to online advertising, marketing and promotion.

FTC Ad Law Blog: A former investigator for the FTC, attorney William Rothbard blogs and provides industry alerts about everything FTC.