BRAND INTEGRITY

6 Affiliate Marketing Pitfalls and How to Steer Clear of Them

CAKE

OPTiZMO™ Technologies

A brand is a company's promise to its customers and includes all the ways a company's image is established. Strong brand integrity has the power to accelerate an organization's growth. That influence is worth protecting.

OVERVIEW

Brand integrity is of significant importance for advertisers and affiliate networks alike. Through affiliate marketing, both have invested large amounts of time and resources to promote, advertise, optimize, and monitor their brand, plus to foster key relationships.

In the case of affiliate marketing, this means relationships with all partners including advertisers, networks, publishers, and affiliates. Trust among all of these partners is key, as how they're closely connected is essential for affiliate marketing success.

With so much at stake, it makes sense that advertisers must protect the integrity of their brand – or in the case of networks, the advertisers they work with, as well as their own - and understand the real risks associated with affiliates who may go rogue.

When advertisers and networks collaborate with the right affiliates, they quickly understand the advantages and benefits. In fact, 90 percent of advertisers think affiliate programs are essential to their marketing strategy.[1] However, an unfortunate disadvantage can be the misuse of a brand through affiliate marketing methods.

How much an advertiser and network invests in their brand integrity sets the foundation for long-term success. You need to consider the possible threats and how your reputation can be impacted by affiliates and other factors. Following are six common pitfalls that can seriously harm a brand and measures you can take to avoid them.

PITFALLS

01 Deviate from brand guidelines

02 Overlook consumer privacy requirements

03 Make bad relationship choices

04 Monitor compliance with manual methods

05 Fail to effectively combat fraud

06 Rely on unstable technology

1

PITFALL

Deviate from brand guidelines

Staying on brand across marketing channels and campaigns enables the growth of your company as well as sets you apart from your competitors.

A strong brand is an imperative asset for an advertiser and its marketing partners.

The purpose of branding is to simply and easily help customers understand what products and services are offered and how they're different from competitors.

A consistent brand strategy helps build loyalty, familiarity, and credibility with current and potential customers. Staying on brand not only plays a vital role in influencing their purchasing decisions, but also creates a sense of trust. Yet, all this could be lost by failing to develop and enforce effective branding guidelines.

How to avoid

The first important step to avoid breaking brand guidelines is to set the ground rules for affiliate marketing campaigns – advertisers need to establish and communicate clear brand guidelines.

These brand guidelines are enforced by terms and conditions (T&Cs) that are shared with networks, which in turn are passed along to affiliates.

Once the brand guidelines and T&Cs are in place, the next essential step includes monitoring and enforcement. If done incorrectly, this can hinder your business. Efficient and effective brand monitoring and enforcement require you to collect and analyze your campaign traffic data.

Leverage data

A performance marketing platform makes it easier to keep tabs on your campaigns, partners, and other activities, so you know precisely how ads are utilized and performing at all times.

Performance marketing or affiliate marketing software should provide reporting on data regarding referrers and other metadata about location, device, operating system, ISP/carrier, language, and user agent. It should also provide features specifically designed to simplify the process of following affiliate marketing brand guidelines.

Data in action

Here are some examples of how to leverage premium software features created specifically for the affiliate marketing industry.
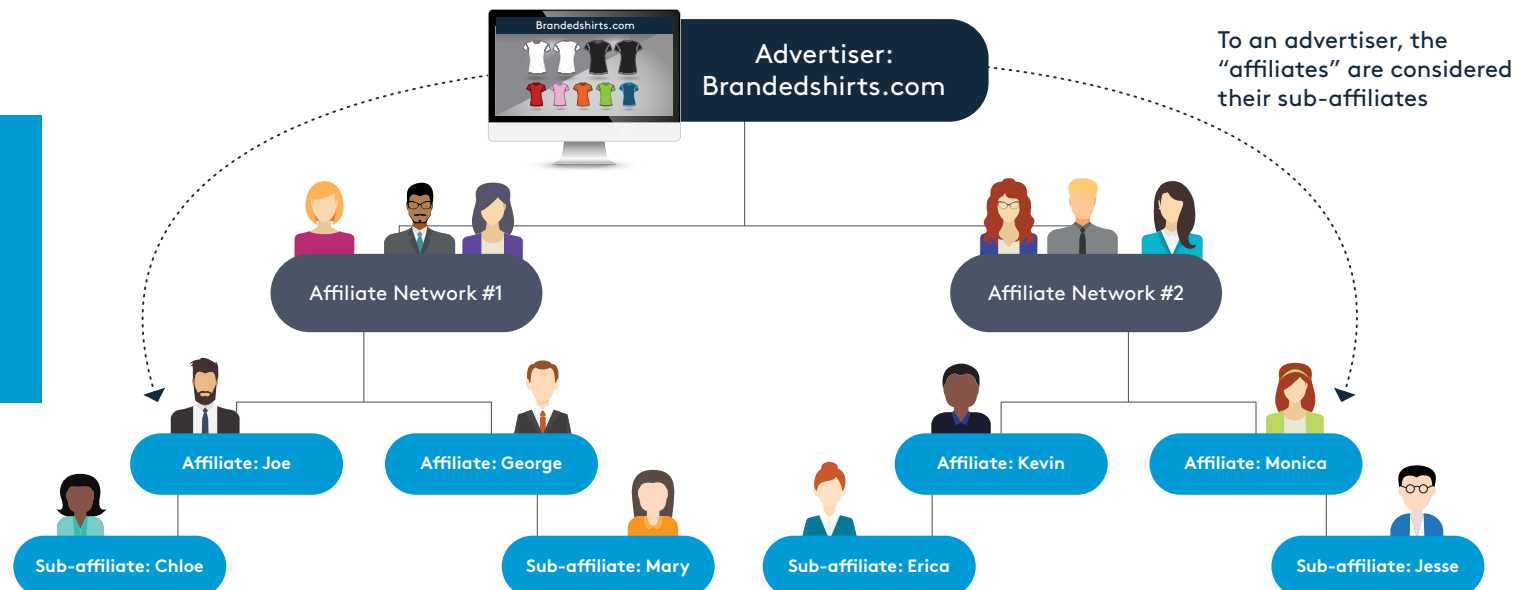
In many instances, advertisers work with networks that have affiliates, and those affiliates often have partners of their own, called sub-affiliates. With sub ID tracking, you can measure sub-affiliate traffic quality and quantity to ensure all of the partners in your affiliate marketing equation are staying in line with your brand guidelines.

Another way for advertisers and networks to enforce guidelines is to clearly communicate offer restrictions and descriptions that are typically found within an affiliate portal and are an extension of the T&Cs. For example, provide affiliates with:

→ A clear snapshot of each offer they are approved to run

→ The accepted types of media compared to those that are not permissible

→ Any other specific requests or requirements from the advertiser

Affiliate Marketing Ecosystem

Advertiser: Brandedshirts.com

To an advertiser, the "affiliates" are considered their sub-affiliates

Affiliate Network #1

Affiliate Network #2

Affiliate: Joe

Affiliate: George

Affiliate: Kevin

Affiliate: Monica

Sub-affiliate: Chloe

Sub-affiliate: Mary

Sub-affiliate: Erica

Sub-affiliate: Jesse

5

2

Overlook consumer privacy requirements

Consumer privacy

is more important

than ever.

If poorly handled,

it can negatively

impact a brand

and result in

hefty fines.

Data privacy matters to consumers and deserves a high place on the priority list, especially when it comes to affiliate marketing and brand integrity.

In fact, safeguarding consumer privacy and security are a "potential source of competitive advantage that may be a central component of brand-building and corporate reputation," according to a Deloitte report about consumer trust and data protection.[2]

With affiliate marketing programs, another layer of complexity is added when it comes to data collection and privacy. In the highly interdependent affiliate marketing world of advertisers, networks, and affiliates, huge amounts of data are collected and partners deploy various ways of handling personally identifiable information (PII) for consumers. This intricate network with vast amounts of data, plus recent advancements in consumer privacy laws, adds up to mean a serious commitment to consumer privacy is required.

How to avoid

Procedures and protocols are designed to ensure that all partners abide by relevant data privacy laws and regulations to avoid fines, as well as to protect a brand and reputation. Best practices include:

Look to the experts

Appoint a data protection officer (DPO) to oversee your entire data privacy and security strategy and processes. This is actually required under the European Union's General Data Protection Regulation (GDPR).

Another option is to engage with an outside company or consultant that provides expertise on data privacy to evaluate your current data policies and procedures, and delivers recommendations on ways to enhance them for improved compliance efforts.

Don't fall into the "set it and forget it" trap

Of course, procedures and protocols must be created and put in place to address all the relevant laws and browser initiatives that impact consumer privacy. However, it's also key to regularly audit your system to stay updated with all regulations, as they are constantly evolving.

What happens if you don't comply? Along with a bad reputation, hefty fines can also be issued. For example, GDPR fines can equal up to $20 million euros or 4 percent of a firm's annual global turnover.

Keep everyone aligned in your affiliate marketing ecosystem

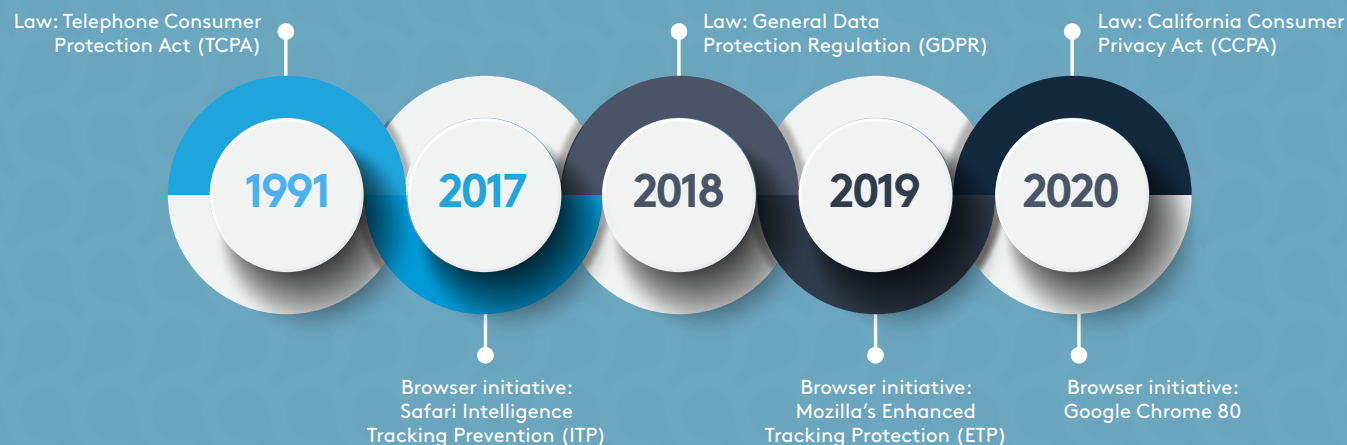Within the T&Cs, include the acceptable use policy for the collection and sharing of PII from the affiliate program. This keeps all partners accountable.

Also, be transparent with your leads about the data you collect and how it will be used for engagement. For example, with email marketing campaigns, leveraging subscription preference centers as part of your opt-out process can provide consumers with more control over their relationship with your brand and the types of communication they want to receive from you.

Know the law

Regulations that govern the collection of PII have been passed by countries around the globe, as well as individual states in the U.S. Ensure all of your affiliate agreements comply with the laws and the privacy policies that apply to those regions.

Below is a timeline of consumer privacy policies, including laws and browser updates. It's important to understand these existing regulations, and also to be aware of new initiatives as they develop.

Law: Telephone Consumer Protection Act (TCPA)

Law: General Data Protection Regulation (GDPR)

Law: California Consumer Privacy Act (CCPA)

1991 **2017** **2018** **2019** **2020**

Browser initiative: Safari Intelligence Tracking Prevention (ITP)

Browser initiative: Mozilla's Enhanced Tracking Protection (ETP)

Browser initiative: Google Chrome 80

3

PITFALL

Make bad relationship choices

In the affiliate marketing ecosystem, the partners you associate with influence your overall reputation and credibility which could strengthen, or unfortunately hurt, your brand integrity.

Your relationships – with affiliates, sub-affiliates, and other networks – can make or break your reputation. They have the potential to positively impact your brand integrity, but they also have the ability to tarnish your brand with customers and other players in the affiliate marketing ecosystem.

You need to trust your partners are abiding by your guidelines, as well as following other regulations, which can be numerous and varied. Many industries that leverage affiliate marketing - such as finance, education, retail, and pharmaceuticals – are highly regulated by organizations such as the Federal Trade Commission (FTC), Securities Exchange Commission (SEC), and individual regulatory bodies per industry.

Most regulations treat affiliate marketing partner activities as if they were conducted directly by the advertiser. This means partners fall under advertisers' responsibilities with affiliate marketing and the advertiser's reputation is on the line if they fail to educate, monitor, and halt a partner's damaging behavior.

In summary, with all of the players in the ecosystem that can affect a brand, you need to monitor all affiliate marketing activity to identify the good versus bad relationships.

How to avoid

Steer clear of bad relationship choices by implementing a two-step process to protect a brand's integrity. This includes finding the right partnerships, then effectively and consistently managing them.

Identify partners that are the right fit

→ **Industry events** - Meet affiliates in-person at industry conferences, such as Affiliate Summit, MailCon, Affiliate World, India Affiliate Summit, and many others, to understand their business goals and build a true partnership that is mutually beneficial.

→ **Affiliate networks** - For advertisers, leverage an affiliate network to meet potential partners and establish relationships.

→ **Social media groups** - Join leading Facebook and LinkedIn groups to gain insights about potential good and bad partners.

Nurture healthy relationships

→ **Ethics** - Work with affiliates who follow regulations, abide advertiser and network requests, and reward partners accordingly. As the advertiser or network, you can offer higher cost per acquisitions (CPAs) for affiliates who drive the best-performing traffic as an incentive and to nurture long-term relationships. And conversely, eliminate low-value and poor-performing affiliates altogether.

→ **Communication** - Include a two-way feedback process between you and your partners. For example, advertisers should share conversion data with the network or affiliate partners to optimize the affiliate's promotional efforts. On the flip side, affiliates should share the content of their promotions with the advertisers and networks.

→ **Technology** - Leverage software to streamline and monitor the creative distribution process. For instance, performance marketing software allows advertisers and networks to upload approved creatives, making it easily available for all affiliates to download.

→ **Commitment** - Realistically, traffic and sales will likely experience peaks and valleys, and other fluctuations over time. However, if a partner demonstrates a true effort to optimize the campaigns, it may be worth investing in that partnership and overcome challenges together. When partners share this core belief, the results can equal a relationship built on a long-term, mutually beneficial outlook.

4

PITFALL

Monitor compliance with manual methods

Effectively tracking compliance is a necessity to develop a successful affiliate marketing program. This is where automation outperforms manual processes.

Attempting to manually track all of your affiliate partners is a huge pitfall. Effectively monitoring affiliates poses a challenge for running a small affiliate program, but becomes exponentially more demanding, time consuming, and resource-intensive as a program grows.

When affiliates fail to comply with brand and privacy guidelines, and legal regulations either purposefully or accidentally, it is difficult to use manual processes to identify and mitigate these non-compliance issues. Ultimately, advertisers and networks may be held accountable for this, which can lead to large fines.

For example, the CAN-SPAM Act is a law pertaining to email marketing which requires that marketers provide consumers with a method to opt out of future email marketing campaigns and define a set of requirements for acceptable email marketing practices. Violations of the CAN-SPAM Act can generate penalties of up to $43,280 per email if found to be non-compliant.

These are convincing reasons why it can be seriously risky to rely on manual tools such as spreadsheets and email trails to track and monitor affiliate compliance.

How to avoid

Leveraging a third-party platform and/or multiple automated solutions can save significant resources and deliver an effective strategy for affiliate compliance monitoring across all channels. Some of these platforms can also make it easier for affiliates to stay in compliance, by putting all the resources they need in one central location. For email marketers, this would include items such as opt-out links, suppression files, and approved creatives. Let's deep dive into a specific channel to examine the importance of compliance and best practices.

When it comes to email affiliate programs, specific challenges arise that require advertisers to take various measures that ensure all partners follow brand guidelines and other regulations, such as CAN-SPAM.

For instance, advertisers that leverage affiliate networks to facilitate their marketing programs can easily expand to hundreds of email affiliates, also referred to as mailing partners. This makes manual monitoring and management of your compliance program effectively impossible for just about any advertiser or network.
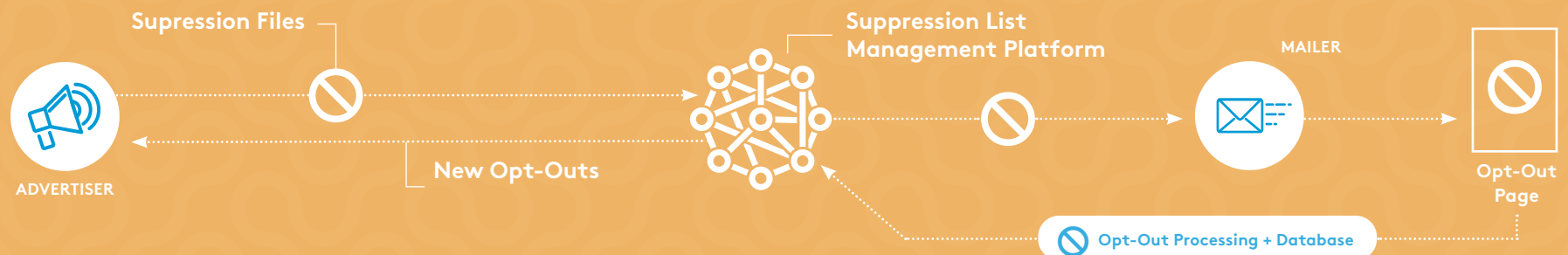
Engaging with a third-party, automated suppression list management platform provides an easy-to-use and scalable solution to automatically track compliance within your email program, while also making it easier for your affiliates to maintain compliance.

Another bonus: Using an industry leading partner helps demonstrate your commitment to compliance and also helps further mitigate your risk if an affiliate does become non-compliant. It's like an insurance policy for advertisers. Following is a basic step-by-step guide for ensuring compliance:

1. Prior to each affiliate mailing, provide a unique opt-out link and an updated suppression file of opt-outs and any other files you want suppressed.

2. Collect new opt-outs the affiliate generates, then process and add them to the updated suppression file.

3. Redistribute the updated suppression file to your mailing partners for future campaigns.

4. Repeat after every campaign and mailing.

5. Multiply this by the number of affiliates in your program and the number of mailings they generate, and the numbers and effort can grow exponentially.

It's easy to see that manually managing this type of email compliance program can be challenging with even one email affiliate, but becomes extremely difficult as more affiliates are added. The challenge to manually monitoring a program like this is not just in the time and effort, but also in the very real likelihood for human error to create a potential compliance issue. This is why few companies attempt to manually manage their email compliance programs once they add mailing partners to the mix.

EMAIL SUPPRESSION LIST MANAGEMENT

Supression Files

Suppression List Management Platform

MAILER

ADVERTISER

New Opt-Outs

Opt-Out Processing + Database

Opt-Out Page

5

Fail to effectively combat fraud

While affiliate marketing is a proven, data-driven model that drives traffic and increases sales, it also attracts fraud that can damage a brand.

Affiliate fraud is a top concern in the affiliate marketing industry and for good reason. Affiliate marketing has already generated $15 billion in revenue in 2020, but at least 9 percent of all these transactions were affected by fraud.[3] This is a red flag, and your organization's revenue and reputation are at risk when fraudsters seep into your affiliate marketing program.

Fraud takes various forms, including malicious browser extensions, mobile app install fraud, fraudulent purchases, click fraud, and more. In whatever form, the end result is that fraudulent affiliates steal attribution on conversions and receive undeserved payments.

Strong affiliate marketing programs reward affiliates who promote brand integrity and bring in customers through legitimate pay-for-performance methods. It's important to make sure these affiliates receive their correct payouts, as well as to detect fraudsters in real-time.

How to avoid

An effective fraud management process ensures that acquired sales are authentic, valid, and profitable. Furthermore, it enhances advertiser and affiliate relationships by building trust and transparency.

To identify fraudulent traffic, advertisers and networks must leverage technology to capture, monitor, and analyze granular data about clicks and conversions.

With insights provided by data, you can identify fraud in real-time as well as block high-risk traffic based on changes in affiliate performance data.

How is this accomplished? Here are some features to look for in a performance marketing platform and specific actions to combat fraud:

Alerts — Alerts are customizable, time-sensitive notifications that help you quickly catch fraudulent activity and stop it at the source. Set up alerts for suspicious behavior such as:

→   Excessive clicks, conversions, login failures, click-to-conversion ratios and/or duplicate IPs

→   Affiliate login outside of sign-up radius

→   Landing page modifications

Reports — Reports identify real-time trends based on your data and provide actionable insights for you to optimize your campaign performance. To identify questionable patterns, a good best practice is to frequently review the following reports:

→   Referrer report - Provides the website domains and applications referring traffic to your website. This type of report can be leveraged to pinpoint spam traffic, uncover new or unknown traffic sources, and measure high-and low-performing referring websites.

→   Pixel log - Displays every conversion pixel attempt, whether the conversion is successful or not. It should include details about the pixel attempts, including the IP address of where the conversion pixels are being fired from. The pixel log can help detect fraud by showing potential patterns of IP addresses of bad actors. A pixel log can also identify the threat of automated systems attempting to create conversions using fake information.

Traffic control — Traffic control protects you from click bots and unsecure IP traffic, plus filters out fraudulent referrer traffic which can skew the data with unwanted URLs. Here are some tips for traffic control:

→   Apply low caps, or limits, to new affiliates that only allow them to drive a certain amount of conversions per day to begin. This provides a way for the advertiser or network to analyze the data and ensure its legitimacy with minimal risk.

→   Identify criteria that could resemble bot behavior. For example, if it takes a human 30 seconds to fill out a lead form, but a form is submitted in under 30 seconds, this could indicate bot behavior. A performance marketing platform should include the ability to reject conversions based on customizable minimum time-to-conversion criteria.

6

Rely on unstable technology

Be prepared for growth by relying on stable technology from providers with a strong success track record.

When it comes to affiliate marketing programs, leveraging stable technology instills trust and sustains business continuity, which helps build brand equity.

However, stable technology goes beyond trying to maintain a bug-free system. It also encompasses a solid infrastructure to avoid downtime, as well as the assurance that the technology provider will be available to assist with day-to-day support and be around for the long run.

Imagine two nightmare scenarios – one related to a software provider going out of business; another about unstable technology.

You depend on a cloud-based solution to run your daily business operations. Then with no warning, your SaaS provider announces that it will be closing soon due to bankruptcy. This leaves your company with a limited amount of time to salvage all data, processes, and other things from this particular provider. It could also mean a pause in your company's own operations with partners, which could be catastrophic for your business.

On the technical side, what happens if your company is depending on unstable technology to manage its affiliate marketing programs and this results in downtime? According to Gartner, downtime averages thousands of dollars per minute.[4] And that's just lost revenue. Downtime triggers a chain reaction that can also lead to lost productivity, ruined partnerships, recovery expenses, and intangible costs like reputation and brand damage.

How to avoid

Fortunately, both of these business and technology scenarios can be avoided by choosing your technology partner wisely.

4. Gartner

Look at business stability

The logical way to avert the crisis of handling the fallout of your SaaS provider going out of business is to make sure it never happens in the first place – partner with a stable technology provider from day one. But that is easier said, than done. While cloud-based technologies are a fast-growing sector, the fact is that 25 percent or more of these go out of business within the first couple of years.[5]

Here are ways to check on a technology provider's viability for the long-term:

→ **Traditional vetting** – Start with the basics and do research on the company's history. Check for healthy financial statements, strong financial backing, and business growth.

→ **Reviews** – Make sure the provider has a strong track record of satisfied customers and partners. Resources can range from customer case studies to referrals and recommendations from industry peers. Other useful resources include review sites such as G2 Crowd, Capterra or other industry forums, or simply ask the provider for references.

→ **Service-level agreements (SLAs)** – SaaS providers offer SLAs, which guarantee specific uptime and other terms of access. This is a must-have and be sure to review the terms carefully to confirm you're covered.

Consider technology stability

It's also critical to depend on stable technology platforms across your affiliate marketing technology stack. The consequences of unreliable technology and downtime are more preventable if you depend on platforms that prioritize architectural and infrastructural stability.

→ **Architectural** – When evaluating the architectural stability of a technology provider, look for companies that have solid processes and procedures in place to ensure code integrity. For example, they should have certifications such as Type 2 SOC 2 compliance. SOC 2 is an audit designed to verify that service providers are properly managing data, in the interest of both the organization and clients.

→ **Infrastructure** – Your technology provider should protect you from downtime which typically indicates data loss. While it's nearly impossible to entirely mitigate the threat of downtime, there should be a hierarchy of protocols for efficiently and effectively handling these types of situations. For instance, in the event of a server outage, your technology provider should be able to pivot in real-time to a new set of servers, globally if needed, so that the level of downtime is virtually undetectable to its customers.

Conclusion

Protecting brand integrity is essential for affiliate marketing programs, and requires an investment in time and resources as well as the knowledge of pitfalls to avoid.

Technology is key too. Gathering and monitoring data with reliable and stable technology platforms increases the value of performance marketing campaigns and protects brand integrity, from the initial click to the final conversion. Without insights provided by technology solutions, there's the potential to lose profit, jeopardize relationships, and run into consumer privacy issues.

Overall, managing affiliate marketing programs with data-driven insights and diligence, plus setting up safeguards to avoid the dangerous pitfalls of affiliate marketing.

The results – better partnerships, more revenue, and stronger brand integrity.

CAKE, a global provider of performance marketing software, empowers more than 500 advertisers, networks, and publishers to manage, measure, and optimize their digital marketing campaigns, in real-time. Established in 2010, the company specializes in providing solutions for affiliate marketing, lead generation, and multichannel marketing. CAKE is headquartered in Newport Beach, California with operations in London and New Delhi.

To learn more about CAKE's Affiliate Marketing software, request a demo here.

OPTIZMO Technologies is the recognized thought-leader in the email and online marketing space for email suppression list management, email campaign management, data management, and risk mitigation services relative to email compliance. With an expert staff in pursuit of unrivaled efficiency, innovative technology, and an insatiable desire to problem-solve, clients find a customer-centric business model that not only enhances the way OPTIZMO clients do business but drives the company forward. The company is headquartered in Austin, TX, and has offices and team members in Charleston, Denver, and Brisbane, Australia.

To learn more about OPTIZMO's Email and SMS suppression list management platform and request a demo, click here.