



THE PERILS OF GOING CHEAP:

WHY YOU SHOULD ONLY WORK WITH AN EMAIL
DATABASE SERVICES PARTNER YOU TRUST



Like a fabulously high match rate, a fabulously low price for email appending or list hygiene services calls for a reality check. Top-quality database services don't come cheap. The value a vendor can add to your database direct correlates to their expertise, experience, and investment in technology, as well as the strength of their commitment to regulatory compliance, best practices, and high ethical standards. Vendors who cut corners may be able to charge less than a premium provider, but the true cost of their services can far exceed your initial investment and, worse yet, can potentially bring down your entire email marketing program.

This paper will outline key areas where the services of cheap vendors tend to fall short as well as the risks their shortcomings pose to your email program and your business as a whole.

1. Data Sources

Disreputable vendors obtain data by any means necessary. That includes using Web scrapers (a CAN-SPAM violation), making up email addresses, misleading Web visitors to capture their information, and buying third-party lists that are riddled with spamtraps. Whether they're illegally collected, undeliverable, bogus, or toxic, the bad addresses in a vendor's database can have devastating repercussions for your business. The potential costs include blacklisting and blocking, as well as thousands of dollars in fines for each message you send that violates the law.

To avoid these pitfalls, first-rate vendors license data only from trusted sources that use legitimate, opt-in collection methods. And careful vendors pay only for data that performs, so their sources have a vested interest in providing email addresses that are safe, deliverable, and genuine.

2. Matching capabilities

An email append from a database partner whose matching algorithm is too loose can spell disaster for your marketing efforts and your good name, as you risk getting email addresses that don't belong to your customers. A phonetic matching system, for instance, may append the same email address to a host of different but similar-sounding names. While this practice can raise your match rate, those incorrect matches not only increase the cost of sending your email campaign but can also unleash a barrage of spam complaints. The same is true of household match logic that disregards apartment numbers. You might end up with email addresses for dozens of Smith households in a 600-unit apartment building when you're only interested in the Smiths in apartment 30B.

In contrast, vendors with the technical savvy to develop sophisticated proprietary algorithms are equipped to deliver accurate email addresses for specifically targeted households. Sophisticated vendors also offer individual-level matching, which is critical for financial institu-

tions, healthcare providers, and other organizations that send sensitive or highly targeted communications.

Strict individual matching is even more crucial for updating invalid email addresses. The only accurate method of doing this locates the required information in an exact-match, change-pair email database, which precisely tracks an individual's old and new email address. Vendors without this matching capability perform a reverse append on the bounced email addresses through their appending database to find the customers' names and then run an append to find a different email address than the one they started with. This error-prone process produces loose or household matches, which results in mailings to the wrong individuals.

Finally, an experienced provider should be matching your file against multiple sources to ensure it's covering the available universe of opt-in data. But again, less reputable vendors have even scarier data partners so this is another place where their commitment to regulatory compliance, best practices, and high ethical standards is paramount.

3. Data security

The security of your data should be of paramount concern when choosing a service provider. An unscrupulous vendor could steal your database and rent or sell your priceless customer information a hundred times over. Even honest vendors can put your data at risk if they fail to invest fully in the necessary technology and security practices.

Safeguarding your company information from the constantly evolving tools and techniques of cybercriminals requires the full range of advanced technology, from fail-safe data transfer tools and firewalls to state-of-the-art anti-virus, anti-spyware, and anti-malware tools. A trustworthy, knowledgeable, and vigilant staff is equally essential, as often data thefts have human factors as their root cause. Smart vendors routinely hire unbiased third-parties for security probing and auditing. A top-of-the-line provider will conform to ISO 27000 standards, a globally recognized set of best security practices that incorporate continuous feedback and improvement activities to head off emerging threats.

When your email database services partner has completed its work, make sure all traces of your data are destroyed. If your vendor doesn't have a written data destruction policy, and isn't routinely having hard drives shredded, it is time to find another vendor. Whether it's caused by a malicious attack or employee negligence, a security breach that exposes your subscribers to spamming, phishing, and identity theft can cause major financial losses and irreparable harm to your image and customer relationships.

4. Data Confirmation

Typically vendors deploy a mailing that provides each recipient with the opportunity to opt out of future email communications. Email appending vendors who knowingly deal in low-quality data may simply skip this step or outsource the



process to a company that routinely sends out spam. If that company is blacklisted, the confirmation messages it sends out will simply disappear into cyberspace. The vendor can then spin the lack of responses as evidence that the addresses they're providing are valid, leaving the client with a list full of risky addresses.

Compared to an opt-out mailing, an opt-in mailing is more likely to build goodwill with customers and ISPs. After the confirmation mailing, a capable provider will return your opt-in, opt-out, and non-responders, while using ISP feedback loops to monitor customer complaints. By identifying bad addresses and spam complainers, this process can help you refine your list to avoid blocking and blacklisting. It also reveals your recipients' level of engagement, enabling you to target your communications appropriately.

5. List Hygiene

Some vendors intentionally skip critical hygiene processes to maintain their inflated match rates. Others simply lack the resources and expertise needed to properly filter out deliverable-but-toxic addresses. ISPs are not only adopting more aggressive filtering techniques, but also increasingly using abandoned email addresses as spamtraps. Repeatedly emailing these dormant accounts can prompt anti-spam organizations to blacklist your IP address.

As a number of major retailers who were blacklisted in 2012 discovered, spamtraps can also creep into your database as

email address typos. Your emails could be blocked for weeks or months as a result. Undoing the damage can be equally costly. The stringent terms and conditions for removal from blacklists can reduce a list of millions of email addresses to a few hundred thousand. In comparison, the price of state-of-the-art hygiene services seems negligible.

Simplistic 'email validation' services (e.g. pinging or SMTP checks) fail to identify disposable domains, role accounts (i.e. info@), spamtraps, frequent complainers, and other deliverable but undesirable addresses that can ruin your reputation with ISPs. A careful SMTP check can be a useful tool but it's just one small part of a comprehensive list hygiene service. A more rigorous approach to list hygiene also increases the proportion of good addresses on your list by correcting formatting and syntax errors. Vendors with advanced real-time correction capabilities can even fix typos at the point of registration.

6. Business practices

Unlike providers who work hard to build long-term relationships with clients, shady vendors have no qualms about providing bad addresses or reneging on contracts. When you request a refund, they may insist you accept a credit on a future job, an offer you're bound to refuse based on their shoddy work. Your only recourse may be an expensive lawsuit. Worse still, the company you hired may deprive you of that option by simply vanishing into the ozone.

To avoid getting burned, be on the lookout for red flags. Make sure the vendor's website lists the company's principals and that their headquarters address isn't a post office box or a parking lot in Florida. But don't be fooled by the appearance of legitimacy. Vet a prospective vendor's references at least as carefully as you would those of a new hire. Choosing an unethical vendor could turn out to be the most expensive mistake you ever make.

7. Expert Advice

The value you get from your database services provider extends well beyond the matching and messaging activities required for the project. A trusted vendor will be a committed partner in your success, and provide expert advice throughout the relationship. Cheap vendors don't invest in knowledge-building or senior staff, and aren't in a position to provide consultative, strategic discussions, innovative ideas, or the level of service you may require.

The Bottom line

When choosing a partner to help you optimize your online marketing program, it's important to remember that the quality of email data varies significantly from vendor to vendor. The opposing view of email data as an undifferentiated commodity where upfront costs rule can tempt marketers to overlook the hidden costs of an unreliable vendor's bargain basement deal. A trustworthy provider is your best assurance that your email data will prove to be an invaluable asset to your business and email reputation, your brand image, and... your bottom line.