Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Position on Selling Email Address Lists

June 2019, Version 1.01
Reference URL to this document: www.m3aawg.org/SellingEmailLists

The practice of selling, buying or sending to lists of purchased email addresses – whether business to business (B2B), business to consumers (B2C) or other categories, is in direct violation of M³AAWG core values. There are many reasons why buying and selling of email address lists is an abusive practice. It leads to a high volume of non-permission based email and creates a drain on corporate resources.

Trafficking in third-party email lists generates significant risks of violating consent requirements in privacy and anti-spam legislation all over the world. It also frequently abuses the Terms and Conditions of most reputable email sending platforms.

There is a widespread and persistent belief among email marketers that permission is not necessary when sending email to business addresses – that is, email addresses used as part of a business entity. This belief is perpetuated because many B2B senders face very little consequence for their poor list collection practices. Many business addresses do not have Feedback Loops (FBLs) so complaints are always low. Numerous corporate domains will block all mail if the list source is suspect, and these blocks may not only be abrupt, they may also deny mailbox entry for extremely long periods.

Even hosted business mail, like Office 365 and G Suite by Google, which have FBLs for their consumer mail, do not have FBLs for their business hosting. Spamtrap networks are also limited when it comes to business addresses. Due to the lack of outside signals, senders of purchased business lists face few consequences because the ESPs (Email Service Providers) hosting these senders must rely mainly on direct user complaints to detect non-permission practices.

While this belief has been reinforced throughout the marketing sphere, the position of M³AAWG is the opposite: Permission is required regardless of whether the mail is B2B or B2C.

Privacy Regulation Concerns

In an era of email and privacy regulations, which are protecting consumers from unsolicited marketing and misuse of data, there is a perception that those protections do not extend to business email addresses. The European Union's General Data Protection Regulation (GDPR) and Canada's Anti-Spam Legislation (CASL) do not differentiate between B2B or B2C – an email address is an email address – with the accompanying permissions. There is no difference between myfirstname@gmail.com and myfirstname@corporate.com email addresses. Both can be used as personal and corporate or business email addresses because they ultimately point to an individual that is covered under GDPR or CASL.

However, CASL includes detailed conditions that need to be met when sending to a third-party list. Under these regulations, recipients must expressly consent to the source that they have given permission to share their email addresses with third parties. All companies are accountable for managing the recipient's consent and unsubscribe requests, and must include their identification and unsubscribe mechanism in each commercial email. Other specific conditions also apply that are detailed in the CASL regulations.

Error Prone Data

The data exchanged by email list vending services is error prone. The collection methods and list segmentation, classification, and identification by such vendors are dubious at best. There is seldom, any knowledge by the email address owners that their personal property is being bought and sold, and therefore there is no permission basis at all and no way to revoke permission. After all, who would willingly enter their email address if they knew that it was bound to be distributed to anyone willing to pay someone else for it?

When a person gives a company, a group, or an individual permission to market to him or her, that permission is provided exclusively to the party in question. It is not transferable to other parties despite contracts or payments in place. This permission applies to email addresses of individuals and of group aliases, and it applies whether the address is used for business or for non-business purposes.

Permission must also be revocable by the address owner. This must be accomplished with reasonable effort with the organization to whom permission was granted – this is the normal "unsubscribe" feature of any legitimate mailing list. Such revocability is impossible as soon as the recipient's address is distributed to a third party, as happens when address lists are bought and sold as commodities. This leaves the end user having to unsubscribe from multiple parties after giving their address to only one.

It is the position of M[3]AAWG that third-party email list sales and purchases are abusive practices and that sending to purchased lists is also abusive, whether B2C, B2B or another objective. Sending email to someone who did not explicitly give informed consent for his or her email address to be used by the sender is never acceptable. It results in innumerable complaints, which further illustrates how much end users find this practice abusive. It also results in delivery issues, largely because of those complaints. Legitimate marketers do not engage in buying or selling email addresses.

As with all documents that we publish, please check the M[3]AAWG website (www.m3aawg.org) for updates.

M3AAWG0125-version 1.01