EMAIL INDUSTRIES

ZoomInfo Deliverability Audit

December 2022

About the Auditor

- Founded in 2008, Email Industries is a pioneering email deliverability consultancy and software-as-a-service provider with more than 85 years of combined domain expertise.
- The company regularly works with many of the world's most respected brands, including Adobe, Mailchimp, and Oracle, to help them improve their deliverability and protect their systems.

Summary

- Email Industries performed a comprehensive deliverability audit of ZoomInfo's email privacy notice program.
- Email Industries found that ZoomInfo has implemented and actively manages best-in-class infrastructure and protocols to facilitate sending privacy notices via email, which exceeds that of most Fortune 500 companies.
- With a few minor exceptions that ZoomInfo addressed following this report, ZoomInfo meets or exceeds industry standards and best practices for deploying privacy notices via email.

Scope

1. Audit the infrastructure and deliverability of ZoomInfo's email privacy notice program.
2. Establish current deliverability benchmarks, practices, and protocols.
3. Grade the program and provide a list of recommendations as needed.

Focus Areas

Focus	Grade	Status
Authentication	A	Completed
Domains	A	Completed
IP Addresses	A	Completed
Bounces	A	Completed
Monitoring	A	Completed
Infrastructure	B	Completed

Authentication

Security

- ZoomInfo's notification deliveries occur in a manner that conforms with industry-recognized best practices, using authentication signals that guarantee the email's legitimacy, such as DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF). These are designed to prevent phishing and forged email attempts by third parties.

Anti-spoofing

- ZoomInfo has implemented an anti-spoofing technology called Domain-based Message Authentication, Reporting, and Conformance (DMARC), which assists in validating the trustworthiness of emails sent.
- Based on the findings in this audit, all policies for DMARC are set to "reject," which instructs the receiver's network to bounce the email message if DKIM or SPF is not passed. This is a highly recommended best practice.

Branding

- ZoomInfo participates in the Brand Indicators for Message Identification (BIMI) project, further authenticating its conformity to DKIM / SPF and DMARC.
- The final process of BIMI certification – receiving a Verified Mark Certificate – is currently underway. Based on what other Email Industries customers have experienced, this process may take several months. It's now out of the control of ZoomInfo.

Domain Alignment

- Link branding in the content of the aforementioned technology (DKIM / SPF / DMARC / BIMI) resolves to a single domain. This domain alignment is considered a best practice to encourage trust with mailbox providers.
- Even though domain alignment has been achieved, it is important to recognize that there is still a possibility that an email does not deliver successfully for reasons outside of ZoomInfo's control. Additionally, a downstream email filter could quarantine email delivery after being accepted successfully by the mailbox provider.

Domains

- Sending from separate domains (e.g., zoominformation.com) is a standard practice used by ZoomInfo and many high-volume senders, which allows its notification emails to be unaffected by marketing or other email communications sent from zoominfo.com.
- All links in the emails are transparent (e.g., no use of link shorteners, such as bit.ly), and all links point back to zoominfo.com for validity.
- To increase transparency even further, in the early stages of this deliverability audit, Email Industries recommended that ZoomInfo remove domain privacy for the notification domains (i.e., make the WHOIS information public) so the contact information is visible and aligns with the information listed on zoominfo.com. To its credit, ZoomInfo implemented this recommendation immediately.

IP Addresses

- Robust sending infrastructure is set up to use multiple static IPs per platform and domain to effectively load balance the notifications and allow ZoomInfo to address possible issues while minimizing the impact of current emails in the queue to be sent.
- All the IPs are set up with proper rDNS, so they resolve to a zoominformation.com or zoominfo-notice.com domain name to validate that the IPs are used for those domains, which is considered to be a best practice.
- ZoomInfo has added additional IPs to help with the volume of notifications that need to be sent and is not planning on removing the existing IPs. This sends a positive and authentic signal to mailbox providers that ZoomInfo is not attempting to circumvent spam filters but rather is improving its infrastructure to handle possible issues in the future.

Bounces

- Hard bounces (i.e., invalid email addresses) are suppressed, as they should be, and not ingested into the system for future notifications to reduce the risk of future deliverability problems, which is an issue that many high-volume email senders have experienced.
- Looking at 30 days of mail logs, from September 1, 2022, to September 30, 2022, there were instances of soft bounces due to reputational issues with mailbox providers. When the audit was completed, those blocks had been resolved, meaning ZoomInfo addressed those issues promptly.
- Soft bounces are retried because of the wide variety of possible issues. ZoomInfo was provided with and is now using a list of server responses for when an address should be removed because of a bad address versus a delivery issue because of reputation at the filter.

Monitoring

- ZoomInfo is continuously monitoring the deliverability of its notification systems using the top-of-the-line email deliverability analytics platform, Everest.
- ZoomInfo has an established process whereby, at the time of possible blocklist or reputation drop, its team will address and resolve what can be mitigated. This includes adjusting sending frequencies, working with mailbox providers, and reaching out to filtering companies and blocklists to identify problems.
- This practice was witnessed when looking at 30 days of logs, from September 1, 2022, to September 30, 2022, and seeing the removal of known blocks.
- To solidify the handling of possible abuse issues, per Email Industries' recommendation, the domain entries at abuse.net have been updated to include the abuse@zoominfo.com mailbox for possible problems at the different providers.

Infrastructure

- Current structure uses an MTA (Mail Transport Agent), which allows ZoomInfo to throttle and expand the structure as they deem fit to address possible delivery issues.
- Email Industries suggests exploring possible alternatives and/or upgrades to its MTA so ZoomInfo can further segment its sending based on mailbox provider and filter. This will allow them to segment the emails with issues without stopping the notifications to others.

Conclusion

It is Email Industries' expert opinion that ZoomInfo meets industry-recognized best practices across all of the critical email-sending protocols and exceeds that of most Fortune 500 companies, in which only 49.9 percent have implemented DMARC and only 3.2 percent have fully implemented BIMI.

DEFINITIONS

A. “Authentication” means a variety of methods that help mailbox providers (e.g., Google) identify email sent by a brand; these methods include DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF), and Domain-based Message Authentication, Reporting, and Conformance (DMARC).
B. “Blocklist” means a list of spammers, typically maintained by an independent organization, used by mailbox providers to determine whether and where to deliver email.
C. “Brand Indicators for Message Identification (BIMI)” means an email standard that lets commercial email senders add a brand logo to authenticated messages sent from their domain.
D. “Bounces” means when a mailbox provider rejects an email because it was sent to an unknown email address (hard bounce) or because of a temporary condition like the recipient’s mailbox being full (soft bounce).
E. “Deliverability” means where an email lands (e.g., inbox, promotions, or spam) once the message is received.
F. “Domain Alignment” means a mechanism that ensures an authenticated email domain aligns with the domain found in the “From” header address, representing the sender’s identity.
G. “Grade” means a letter grade associated with the infrastructure, processes, or performance, where (i) “A” indicates excellent, (ii) “B” indicates good, (iii) “C” indicates satisfactory, (iv) ”D” indicates less than satisfactory, and (v) “F” indicates unsatisfactory.
H. “Link Branding” means all the links in an email point by the brand sending the email (e.g., company.com) instead of the email service provider (e.g., mailchimp.com).