



GET MORE INFO

receiverservices@returnpath.net

1-866-362-4577

The Return Path Reputation Network Blacklist

Make the most accurate decisions about mail entering your network while reducing subscriber complaints.

Return Path's Reputation Network Blacklist is a real-time list of senders categorized as "worst-of-the-worst" based on our reputation data network. Our Reputation Network is an open, collaborative network where data from more than 100 million inboxes is collected. The data in our network powers the Reputation Network Blacklist (RNBL). Leading ISPs have experienced greater than a 25% reduction in complaints after implementing the Reputation Network Blacklist.

Return Path's improved Reputation Network Blacklist currently contains 1-2 million IP addresses. The blacklist is compiled using a behavioral predictive model approach that analyzes more than 600 variables for each sending IP address. This real time scoring model is unique because it scores IP's in real time and incorporates more volume, spam traps, and complaint sources. This comprehensive methodology combined with rapid zone updates (~ every 10 minutes) offers the most current and accurate sender reputation profiles available.

How does it compare to other commonly used blacklists?

Our methodology provides a larger and more comprehensive list, the table below details the comparison:

Blacklist	% Overlap	Reputation Network Blacklist
CBL	73%	27% of IP addresses appearing on the list are not listed by CBL
Barracuda	68%	32% of IP addresses appearing on the list are not listed by Barracuda
PBL	82%	18% of IP addresses appearing on the list are not listed by PBL

What's new and different about the Reputation Network Blacklist?

The blacklist is vastly superior to the 1.0 version based on size, methodology, updates, and scoring:

Feature	Blacklist 2.0	Blacklist 1.0
Size	1-2 million IP addresses at any given time	100,000 – 200,000 IPs at a time
Methodology	Behavioral Predictive model, analytically driven using more than 600 variables to analyze IP patterns	Rule-based decision tree with limited interaction between variables
Updates	Updates in real time, as queried; transferrable zone file updates every ten minutes	Updated once every four hours
Scoring	Scores every IP both when queried and when data is received	Scored only those IPs which send significant volume to contributing ISPs
Platform	Built on RTS data and modeling platform to easily handle more requests per second with simple hardware scaling	Stand alone product; not built on data platform
Support	Fully staffed customer support desk with a new ticketing system; human response to every inquiry with specific information regarding the listing reason.	Fully staffed customer support desk; human response to every inquiry with specific information regarding the listing reason.

What variables are used to compile the blacklist?

Our predictive model looks at 600+ variables, see below for a sample:

- Delivered rate and quantity: How much mail from this IP address was sent and delivered successfully to inboxes.
- Rejected rate and quantity: How much mail from this IP address was sent and blocked outright (at the gateway).
- Filtered rate and quantity: How much mail from this IP address was sent, accepted by the MTA, but then filtered into a “junk” or “spam” folder.
- Unknown user rate: How much mail from this IP address was addressed to invalid recipients, and therefore rejected.
- Complaint rate: How much mail from this IP address was reported as spam by recipients, with appropriate safeguards against outliers and gaming.
- Spam trap hits: How much mail from this IP address was addressed to our spam trap network (addresses which have never sent or requested any mail, operated either by Return Path or our data partners)

Where does Return Path get the reputation data to build the blacklist?

All receivers (ISPs and filtering companies) who participate in Return Path’s Reputation Network contribute “reputation data” that Return Path analyzes to power the blacklist and other tools to quickly and accurately separate the good senders from all the rest. The requested data is non-confidential, based entirely on aggregate analysis of sender activity. We require no subscriber-level information. Currently, data from more than 100 million inboxes is collected.

How is the blacklist customized for my network?

Our blacklist model relies on your actual network data along with others who contribute data so the blacklist blocks the traffic that causes the most serious problems for your network. Any sender generating abnormally high complaints, unknown users, hitting spam traps, etc. on your network is automatically listed on the blacklist. Therefore, the list is customized to your mail traffic patterns and particularly effective in blocking known problem senders.



How are inquiries from blocked senders handled?

Return Path provides information on www.senderscore.org for senders who are blocked based upon the blacklist data. This site allows senders to research their reputation scores and understand why their IP address(es) are listed. Senders can also request temporary removal from the blacklist if they have found and fixed the underlying cause of their poor performance. Finally, senders can submit additional inquiries by email that are handled by a fully staffed customer support desk. All inquiries receive a detailed human response that identify issues and recommend solutions.

How are senders removed from the blacklist?

When a sender fixes their email sending problems, they are automatically removed from the blacklist. In addition, a sender can request an immediate, temporary removal while they investigate and work to improve their reputation.

How do I access the Reputation Network Blacklist?

You can query the blacklist over DNS or if you are a large email receiver, Return Path can provide rsync access to the DNS zone file. In order to access the blacklist, you are asked to contribute data to the Return Path Reputation Network. Specific details and access instructions are available upon request, please contact: receiverservices@returnpath.net

The Bottom Line

The comprehensive methodology of the Return Path Reputation Network Blacklist combined with rapid zone updates offers the most current and accurate sender reputation profiles available in a blacklist.

