How to Prevent Your Anti-Spam Product From Rejecting NEFs

The Administrative Office of the U.S. Courts has implemented the Sender Policy Framework (SPF) on all of its outgoing e-mail, including Notices of Electronic Filing (NEFs). The purpose of this implementation is to reduce the ability of malicious senders (spammers, phishers, etc.) to forge their mail identity using the mail domains that are maintained by the U.S. Courts. Most anti-spam products, both commercial and open-source, will recognize SPF e-mail headers and therefore prevent NEFs from being tagged as spam.

The implementation of SPF is not foolproof. Some anti-spam products do not utilize SPF and use other means of spam detection. One popular method of spam detection is to subscribe to a list of known malicious senders, or a "blacklist." The U.S. Court's domain has in the past erroneously appeared on these blacklists due to the increasing amount of NEFs being generated from this domain. It is therefore highly recommended that any firms or individuals that maintain their own anti-spam service to add "whitelist" entries for the U.S. Courts domain. This change will allow for successful delivery of NEFs regardless of any blacklisting of the U.S. Court's email domain.

Whitelist entries for U.S. Courts email domains

All NEFs from the Northern District of New York will originate from the following domain: nynd.uscourts.gov. You should also consider whitelisting the entirety of the U.S. Courts mail system with: uscourts.gov

The TCP/IP addresses of the U.S. Courts outgoing email servers are: 208.27.111.0/24 and 208.27.203.0/24.

DISCLAIMER: This information is provided only as a courtesy to filers. Neither the U.S. District Court for the Northern District of New York nor the Administrative Office of the U.S. Courts is responsible for any damages resulting from a misconfiguration of your anti-spam product.