



Domain Name Anti-Abuse Policy

Abusive use(s) of <.fedex> domain names will not be tolerated. The nature of such abuses creates security and stability issues for the registry, registrars, and registrants, as well as for users of the internet. In general, Federal Express Corporation ("FedEx") defines abusive use of a domain as the wrong or excessive use of power, position, or ability, and includes, without limitation, the following:

Illegal or fraudulent actions

- Spam: The use of electronic messaging systems to send unsolicited bulk messages. The term applies to email spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of websites and internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service (DoS) attacks.
- Phishing: The use of counterfeit web pages that are designed to trick recipients into divulging sensitive data such as usernames, passwords, or financial data.
- Pharming: The redirecting of unknowing users to fraudulent sites or services, typically through DNS hijacking or poisoning.
- Willful distribution of malware: The dissemination of software designed to infiltrate or damage a computer system without the owner's informed consent. Examples include, without limitation, computer viruses, worms, key loggers, and Trojan horses.
- Fast-flux hosting: Use of fast-flux techniques to disguise the location of websites or other internet services, or to avoid detection and mitigation efforts, or to host illegal activities. Fast-flux techniques use DNS to frequently change the location on the internet to which the domain name of an internet host or name server resolves. Fast-flux hosting may be used only with prior permission of Public Interest Registry.
- Botnet command and control: Services run on a domain name that are used to control a collection of compromised computers or "zombies," or to direct denial-of-service attacks (DDoS attacks).
- Distribution of child pornography.
- Illegal access to other computers or networks: Illegally accessing computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"). Also, any activity that might be used as a precursor to an attempted system penetration (e.g., port scan, stealth scan, or other information-gathering activity).

FedEx reserves the right to deny, cancel, or transfer any registration or transaction, or place any domain name(s) on registry lock, hold, or similar status, that it deems necessary, in its discretion (1) to protect the integrity and stability of the registry; (2) to comply with any applicable laws, government rules, or

requirements, requests of law enforcement, or any dispute-resolution process; (3) to avoid any liability, civil or criminal, on the part of FedEx, as well as its affiliates, subsidiaries, officers, directors, and employees; (4) per the terms of the registration agreement; or (5) to correct mistakes made by FedEx or any Registrar in connection with a domain-name registration. FedEx also reserves the right to place upon registry lock, hold, or similar status a domain name during resolution of a dispute.

Abusive uses, as defined above, undertaken with respect to <.fedex> domain names shall give rise to the right of FedEx to take such actions.

Abuse point of contact and procedures for handling abuse complaints

FedEx has established an abuse point of contact to help facilitate the review, evaluation, and resolution of abuse complaints in a timely manner. The abuse contact can be reached by emailing ngtld-abuse@cscinfo.com. For tracking purposes, FedEx will utilize a ticketing system with which all complaints will be tracked internally. The reporter will be provided with the ticket reference identifier for potential follow-up.