Domain Name Anti-Abuse Policy

Abusive use(s) of .CFA 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, CFA Institute ("CFA") 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 e-mail spam and similar abuses such as instant messaging spam, mobile messaging spam, and the spamming of Web sites and Internet forums. An example, for purposes of illustration, would be the use of email in denial-of-service 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 Web sites 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)

CFA 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 CFA , 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 CFA or any Registrar in connection with a domain name registration. CFA 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 .CFA domain names, shall give rise to the right of CFA to take such actions.

Abuse point of contact and procedures for handling abuse complaints

CFA 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 e-mailing ngtld-abuse@cscinfo.com. For tracking purposes, CFA 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.