wiley

NEWSLETTER

Six Easy Steps to Firewall Protection against Coordination

July 2006

The Federal Election Commission (FEC) limits the ability of organizations to engage in federal campaign activity through its coordination rules. Organizations are prohibited from, or severely restricted in, making "coordinated communications," as these communications are considered to be in-kind contributions made to a candidate, authorized committee or political party committee. Corporations are flatly prohibited from making these contributions, while political action committees (PACs) are prevented from making contributions in excess of $5,000 per election cycle. In other words, a coordinated communication can be an illegal contribution.

Nevertheless, in recent revisions to its coordination rules, the FEC created a safe harbor for those political committees that construct and implement a "firewall" between coordinating and non-coordinating units operating within the same organization. *See* Coordinated Communications, 71 Fed. Reg. 33,190, 33,206 (June 8, 2006) (to be codified at 11 C.F.R. § 109.21(h)), available at www.fec.gov/law/cfr/ej_compilation/2006/notice_2006-10.pdf. A "firewall," in this context, is a system that prevents coordinating and non-coordinating units in the same organization from sharing information on a candidate, authorized committee or political party committee. Organizations that design and implement an appropriate system will fall under the firewall safe harbor and will have established a rebuttable presumption that their independent campaign-related activities are not "coordinated communications" if performed by non-coordinating persons. Below are six steps an organization should follow to take advantage of the firewall safe harbor.

Authors

Carol A. Laham
Partner
202.719.7301
claham@wiley.law

D. Mark Renaud
Partner
202.719.7405
mrenaud@wiley.law

Step 1: Refrain from Coordination Activity until a Firewall Is Designed and Implemented

A firewall policy should be designed and implemented before any coordinating activity takes place. Without a firewall in operation first, an exchange of information is more likely to occur between coordinating and non-coordinating persons. Communications made before a firewall is implemented are likely to fall outside the safe harbor.

Step 2: Design a Firewall

Generally, a firewall should be designed to prohibit the flow of information between coordinating and non-coordinating persons. Recognizing that the effectiveness of a firewall depends upon an organization's structure, clients and personnel, the FEC did not dictate the "specific procedures required to prevent the flow of information." Thus, what is required to design a proper firewall policy is somewhat nebulous. The FEC, however, provides insight regarding proper firewall policy design through its explanation and justification and through an enforcement matter decision.

Prevent Exchange of Material Information: The safe harbor is destroyed if information about a candidate, authorized committee or political party committee's plans, projects, activities or needs are used by the non-coordinating persons for an independent expenditure or if the coordinating persons convey this information to a person paying for the independent communication (like the PAC of a trade association). The information, however, must be material to the creation, production or distribution of the communication. Any firewall policy should be designed to prevent this exchange of information.

The EMILY's List Factors: The FEC provided insight into what constitutes a sufficient firewall through its decision in Matter Under Review 5506 (EMILY's List). There, a committee's firewall policy prohibited its employees, volunteers and consultants engaged in advertising work from interacting with the candidate, authorized committee or political party committee. These employees, volunteers and consultants also were prohibited from communicating with others in the committee who had direct contact with the candidate, authorized committee or political party committee. Lastly, the committee's firewall policy prohibited employees, volunteers and consultants who had direct contact with candidates or committees from discussing and conveying material information to those employees, volunteers and consultants who did not have direct contact with the candidates or committees who were engaged in non-coordinated advertising efforts. The combination of these measures led the FEC to conclude that the committee's firewall was sufficiently designed to prevent the untoward flow of information between coordinating and non-coordinating entities.

Step 3: Reduce Firewall Policy to Writing

The policy embodying the firewall must be put into written form in order to take advantage of the new firewall safe harbor.

Step 4: Distribute Written Firewall Policy

The firewall policy then must be distributed to all "relevant" employees, consultants and clients affected by the firewall. The term "relevant" includes employees and consultants actually working for the organization that is paying for an independent communication and those engaged in activities with the candidate.

Step 5: Implement Firewall Policy

The firewall policy should be implemented by the organization. Whatever requirements or prohibitions provided in the firewall policy should be followed by the organization's employees, volunteers and consultants.

Step 6: Be Prepared to Provide Information on Your Firewall Policy

An organization that seeks to use the firewall safe harbor should be prepared to provide information about its firewall policy. Information regarding how the firewall operates, when the firewall was implemented and when the firewall policy was distributed to the relevant parties is likely to be required in any challenge to the safe harbor. There is no record keeping requirement in the safe harbor rule, but maintaining the above information will be useful.

In sum, an organization is not required to adopt a firewall policy. In fact, the FEC stated that it will not draw a negative inference from an organization's failure to adopt such a policy. Without a firewall policy, however, an organization runs a greater risk that its independent activities will be deemed "coordinated communications" if persons in other parts of the organization interact with a candidate and his or her campaign. The existence of a firewall goes a long way toward mitigating this risk.