FOLEY

FOLEY & LARDNER LLP

DEVELOPING AN E-DISCOVERY POLICY TO COMPLY WITH E-DISCOVERY OBLIGATIONS

A federal judge recently ordered Qualcomm, Inc. to pay in excess of $8.5 million to Broadcom Corp. due to Qualcomm's failure to comply with its e-discovery obligations arising out of emails and other electronic documents that were not produced to Broadcom. Qualcomm Inc. v. Broadcom Corp., (S.D. Cal.; 05cv1958-B (BLM); Jan. 7, 2008). In addition to the monetary sanction, the court required Qualcomm and its counsel to participate in a Case Review and Enforcement of Discovery Obligations ("CREDO") program. In so doing, the court provided helpful insight into steps companies should take now to minimize the risk of non-compliance with e-discovery obligations, and to develop legally effective and compliant e-discovery policies.

1. **Goals of an E-Discovery Compliance Assessment.** The fundamental goals of an e-discovery compliance assessment in the nature of the CREDO program described in the Qualcomm case are to:

a. Identify potential deficiencies in the existing case management and discovery policies, practices and protocols utilized by the Company, and its in-house and outside counsel.

b. Investigate practices that will prevent failures to preserve and produce electronic and other records required to be produced.

c. Evaluate and test possible alternative policies and practices.

d. Create a Case Management Protocol, including an E-Discovery Policy, for complying with e-discovery obligations.

2. The **Compliance Program** should include the following elements:

a. A **risk assessment** identifying **risk factors** that could contribute to or result in discovery violations, such as

i. **Insufficient communication**, including between the Company and outside counsel, among outside counsel and law firms, and between junior lawyers conducting discovery and senior lawyers asserting legal arguments;

ii. **Inadequate case management** within the Company, between the Company and outside counsel, and by outside counsel;

iii. **Inadequate discovery plans** within the Company and between the Company and its outside counsel;

b. Create and evaluate **procedures, practices and processes** that will correct any deficiencies identified through the risk assessment describe above.

c. Develop and document a **comprehensive protocol** that will minimize, and hopefully prevent, discovery violations. The comprehensive protocol will likely include elements such as:

i. Determining the **depth and breadth of case management and discovery plans** that should be adopted

ii. Identifying by experience or authority the **attorney from outside counsel** who should interface with the corporate counsel and on which issues

iii. Describing the **frequency the attorneys should meet** and whether other individuals should participate in the communications

iv. Identifying **who should participate** in the development of the case management and discovery plans – Company in-house legal, Company IT/IS department and outside legal counsel

v. Describing and evaluating various methods of **resolving conflicts and disputes between the client and outside counsel**, especially relating to the adequacy of discovery searches

vi. Describing the type, nature, frequency, and participants in **case management and discovery meetings**

vii. Identifying required ethical and discovery **training** for all participants

d. The risk assessment and compliance procedures should be **adopted to fit** the Company's particular circumstances, such as when the Company does not have corporate counsel, when the Company has a single in-house lawyer, when the Company has a large legal staff, and when there are two or more firms representing the Company.

e. Identify and evaluate data **tracking systems, software, development of a data map** and procedures the Company can implement to better enable inside and outside counsel to identify potential sources of discoverable documents (e.g. the correct databases, IT systems, archives, etc.).

