CHAPTER 11: TRADE SECRETS AND CONFIDENTIALITY

Trade secret law protects valuable business information that derives economic value from being secret and is subject to reasonable efforts to maintain secrecy. Unlike other forms of intellectual property, trade secrets can last indefinitely as long as they remain secret and continue to provide competitive advantages.

11.1 Trade Secret Requirements

Information qualifies as a trade secret when it derives independent economic value from not being generally known or readily ascertainable by others who could obtain economic value from its disclosure or use, and it is subject to reasonable efforts to maintain secrecy. This definition encompasses a wide range of business information beyond traditional technical secrets.

Economic value can arise from various sources, including cost advantages, improved quality, customer attraction, or competitive positioning. The information need not be complex or revolutionary; simple techniques or processes can qualify if they provide competitive advantages and are not generally known in the industry.

Reasonable secrecy measures demonstrate the owner's intent to maintain confidentiality and help establish the information's secret status. These measures can include confidentiality agreements, restricted access, physical security, employee training, and marking of confidential documents. The adequacy of secrecy measures depends on the value of the information and industry practices.

The subject matter of trade secrets is broader than other intellectual property categories, potentially including customer lists, pricing information, marketing strategies, manufacturing techniques, software algorithms, financial data, and business methods. However, information that is generally known in the industry or readily discoverable cannot qualify for protection.

Reverse engineering represents a significant limitation on trade secret protection. Information that can be discovered through proper reverse engineering of publicly available products generally cannot be protected as a trade secret. This principle encourages innovation while preventing overreaching trade secret claims.

11.2 Misappropriation and Enforcement

Trade secret misappropriation occurs through improper acquisition, disclosure, or use of trade secrets. Improper means include theft, bribery, misrepresentation, breach of duty to maintain secrecy, or espionage, but do not include independent development, reverse engineering, or observation of publicly available information.

The Uniform Trade Secrets Act (UTSA), adopted by most states, provides the primary legal framework for trade secret protection in the United States. The Defend Trade Secrets Act of 2016 created federal

jurisdiction for trade secret cases, allowing owners to choose between state and federal courts while maintaining consistency with UTSA principles.

Remedies for trade secret misappropriation include injunctive relief to prevent further disclosure or use, monetary damages including actual losses and unjust enrichment, and in cases of willful and malicious misappropriation, punitive damages and attorney fees. Injunctive relief is often the most important remedy because monetary damages may be difficult to prove.

The duration of injunctive relief depends on how long the competitive advantage would have lasted if misappropriation had not occurred. Courts consider factors such as the information's useful life, likelihood of independent development, and ease of reverse engineering when determining appropriate injunction periods.

Employee mobility creates ongoing challenges in trade secret law, as companies seek to protect confidential information while employees pursue career opportunities. Courts must balance legitimate business interests in protecting trade secrets against employees' rights to use general skills and knowledge gained through their work experience.

11.3 Best Practices and Risk Management

Effective trade secret protection requires comprehensive policies and procedures that identify valuable information, implement appropriate security measures, and create legal protections through contracts and employment agreements. A systematic approach helps ensure consistent protection and provides evidence of reasonable secrecy efforts.

Identification and classification of confidential information helps organizations focus protection efforts on their most valuable assets while avoiding over-designation that could undermine credibility. Regular audits can identify new information requiring protection and assess the continued value and secrecy of existing trade secrets.

Physical and digital security measures should be tailored to the sensitivity of the information and the organization's operational needs. These measures might include access controls, encryption, secure storage, monitoring systems, and clean desk policies. The level of security should be proportionate to the information's value and competitive sensitivity.

Contractual protections through confidentiality agreements, employment contracts, and vendor agreements help establish legal obligations and provide enforcement mechanisms. These agreements should clearly define confidential information, specify permitted uses, establish return obligations, and include appropriate remedies for breach.

Employee training and awareness programs help ensure that personnel understand their obligations and the importance of protecting confidential information. Training should cover identification of trade secrets, proper handling procedures, obligations under confidentiality agreements, and consequences of misappropriation.