NON-COMPETES, DUTY OF LOYALTY, WORK FOR HIRE, CONFIDENTIALITY AND IP

By Nolan J. De Jong, Esq.

I. SO, ARE NON-COMPETES REALLY ENFORCEABLE?

A. What is a non-compete?

1. A non-compete agreement is a contractual provision in which an employee agrees not to enter into competition with an employer during or after employment.

2. These agreements typically restrict employees from working for competitors, starting a competing business, or engaging in activities that could harm the former employer's competitive edge.

   a. Non-competes often include limitations on duration, geographic scope, and the type of restricted activities.

   b. Non-competes are designed to protect *legitimate business interests* such as trade secrets, confidential information, and client relationships, courts scrutinize their reasonableness to ensure they do not unduly limit an individual's ability to earn a livelihood.

B. Michigan courts take a case-by-case approach to non-compete agreements, assessing their reasonableness in terms of duration, geographic scope, and the protection of legitimate business interests.

1. The Michigan Antitrust Reform Act (MARA)

   a. MARA prohibits unreasonable restraints on trade, meaning overly broad non-competes may be unenforceable.

   b. Courts generally uphold non-competes that protect trade secrets, confidential information, or goodwill but may strike down those that unduly restrict an employee's ability to work.

      i. *Coates v. Bastian Brothers, Inc.* (2007): The Michigan Court of Appeals upheld a non-compete agreement, emphasizing that such agreements are enforceable if they are reasonable in duration, geographic scope, and serve to protect legitimate business interests.

      ii. *Innovation Ventures, LLC v. Liquid Manufacturing, LLC* (2016): The Michigan Supreme Court clarified that non-compete agreements between businesses are not governed by MCL 445.774a, which applies only to employer-employee

agreements. Instead, such agreements must be evaluated under the federal antitrust 'rule of reason' standard, which considers the impact on competition rather than solely protecting business interests like trade secrets or confidential information.

C. The Federal Trade Commission (FTC) rule banning non-competes

1. In April 2024, the FTC issued a rule that would ban most non-compete agreements nationwide, arguing they stifle competition and suppress wages.

   a. Once (and if) it goes into effect, the rule will prohibit employers from imposing non-competes on workers (including independent contractors and unpaid workers), and the ban will extend to all terms or conditions of employment that either "prohibit" a worker from, "penalize" a worker for, or "function to prevent" a worker from either seeking or accepting work in the United States with a different person, or operating a business in the United States, after their employment ends.

   b. In addition to preventing employers from entering into new non-compete agreements as of the effective date, the rule would also require employers to notify non-excepted employees that existing non-competes will not be, and cannot be, enforced.

2. If enacted, the rule will allow existing non-competes with senior executives and in sale of business agreements to remain in force, but it bans new non-competes with senior executives.

   a. A "senior executive" as a worker earning more than $151,164 who is in a "policy-making position."

   b. The narrow exception allowing non-competes in certain "sale-of-business" agreements, includes bona fide sales of a business, of a person's ownership interest in a business, or of all or substantially all of a business's operating assets.

3. Status of lawsuit that is preventing the FTC from enforcing its rule prohibiting non-competes.

   a. Nationwide Injunction on FTC Rule

      i. On August 20, 2024, a federal court in *Ryan LLC v. FTC* ruled that the FTC lacks authority to enforce the rule, issuing a nationwide injunction. The FTC appealed to the Fifth Circuit on October 18, 2024.

   b. Key Findings in *Ryan LLC*

      i. The court held that the FTC exceeded its statutory authority, ruling that the FTC Act does not grant the FTC power to issue substantive competition rules. The rule was also found to be arbitrary and capricious.

   c. Impact of *Loper Bright* Decision

i. The Supreme Court's June 28, 2024, ruling in *Loper Bright* eliminated *Chevron* deference, making it harder for the FTC to defend its rule by requiring courts to evaluate its authority without deferring to its interpretation.

d. Next Steps in Litigation

i. The Fifth Circuit will hear oral arguments after the FTC's Reply Brief is filed on February 24, 2025. The outcome of the appeal could shape the future of the FTC's authority in rulemaking.

D. What does an *enforceable* non-compete look like?

1. Customizing non-compete agreements based on industry-specific risks ensures they remain enforceable while protecting legitimate business interests. For example:

a. Tech Industry

i. A software development company implements a non-compete clause preventing employees who had direct access to proprietary source code and trade secrets from working at a direct competitor within a 12-month period in the same geographic market.

(A) This restriction is narrowly tailored to protect confidential business information without unnecessarily restricting career mobility.

b. Manufacturing

i. A specialty automotive parts manufacturer requires key engineers who develop proprietary production techniques to sign non-competes restricting them from working for direct competitors within a 50-mile radius for 18 months.

(A) This restriction reasonably protects confidential information and prevents unfair competitive advantages.

c. Healthcare

i. A medical practice enforces a non-compete agreement preventing specialist physicians who have built strong patient relationships from opening a competing practice within a 10-mile radius for two years.

(A) This restriction reasonably protects patient retention and business goodwill.

E. What does an *unenforceable* non-compete look like?

a. Tech Industry

i. A software development company imposes a blanket non-compete preventing all engineers, regardless of role or access to trade secrets, from working at any other tech company nationwide for five years. This is overly broad and unlikely to hold up in court due to excessive restrictions on employment.

b. Manufacturing

i. A general assembly line worker is required to sign a non-compete prohibiting them from working at any manufacturing company in the state for three years.

(A) Since the worker does not have access to proprietary processes, this broad restriction is likely to be deemed unreasonable and unenforceable.

c. Healthcare

i. A hospital requires all nurses, regardless of specialization or access to sensitive patient information, to sign a non-compete preventing them from working at any healthcare facility within a 50-mile radius for five years.

(A) This broad restriction excessively limits employment opportunities in a high-demand field and is likely to be struck down as unreasonable.

II. PROTECTING OUR STUFF

A. What is a trade secret versus what is general employee knowledge?

a. Trade secrets include proprietary formulas, processes, customer lists, and other confidential business information that provide economic value by remaining undisclosed.

i. Trade secrets may be protected through confidentiality agreements and enforcement mechanisms to prevent misappropriation.

b. General employee knowledge refers to the skills, experience, and general industry know-how that an employee acquires over time and can take with them to future jobs.

i. General employee knowledge cannot be restricted by a confidentiality agreement because it is not proprietary to the employer and does not constitute a trade secret.

B. What is a confidentiality agreement?

1. Confidentiality agreements outline specific obligations for employees and third parties to prevent unauthorized disclosure of sensitive business information.

    a. Employers must ensure these agreements are narrowly tailored to protect only legitimate business interests without overreaching into publicly available, commonly known industry knowledge or general employee knowledge.

C. How do we make sure employees know the difference between a trade secret and general employee knowledge?

1. Educating Through Training Programs

    a. Regular training sessions help employees distinguish between trade secrets and general industry knowledge.

        i. These programs should include real-world examples, case studies, and interactive discussions to reinforce the differences.

2. Developing Clear Confidentiality Policies

    a. Employers should draft clear and accessible policies that outline what constitutes a trade secret and how employees are expected to handle such information.

        i. These policies should be included in employee handbooks and re-visited during performance evaluations.

3. Implementing Secure Information Management Practices

    a. Restricting access to trade secrets through role-based security, encrypted databases, and internal monitoring ensures that confidential information remains protected and prevents unintentional dissemination.

4. Enforcing Consequences for Breaches

    a. Establishing and consistently enforcing penalties for unauthorized disclosures ensures that employees understand the gravity of mishandling trade secrets.

        i. This may include disciplinary actions, termination, or legal consequences when appropriate.

III. WHAT ARE THE NON-CONTRUCTUAL OBLIGATIONS OF WORKERS?

A. Duty of Loyalty and Good Faith

1. Employees must act in the best interest of their employer, meaning they should avoid conflicts of interest, self-dealing, or actions that undermine the company's operations.

a. It is crucial to establish clear conflict-of-interest policies and provide training on ethical business practices to mitigate risks of employee misconduct.

i. Ensure transparency and disclosure mechanisms that allow employees to report potential conflicts before they become legal issues.

B. Workplace Safety and Compliance

1. Employees have an obligation to follow safety regulations, adhere to OSHA standards, and comply with internal workplace policies.

2. Employers should regularly update safety protocols, conduct training, and perform audits to prevent workplace hazards.

3. Management teams play a key role in enforcing compliance, addressing violations, and fostering a culture of accountability to minimize legal exposure and enhance employee well-being.

C. Confidentiality and Data Protection

1. Employees must safeguard proprietary company information, trade secrets, and sensitive client data, even if they have not signed a formal confidentiality agreement.

2. Implement strong cybersecurity policies, limit data access based on roles, and educate employees about the consequences of data breaches.

a. Employers should establish procedures for handling confidential data breaches and reinforce expectations during onboarding and periodic training sessions.

D. Professional Ethics and Conduct

1. Upholding ethical standards is a fundamental expectation for employees across all industries. This includes honesty in reporting time worked, proper use of company resources, and adherence to professional codes of conduct.

a. Employers must communicate these expectations through codes of ethics, training, and disciplinary procedures to ensure integrity in the workplace.

E. Whistleblower Protections and Reporting Duties

1. Employees who report unlawful or unethical activities are protected under state and federal whistleblower laws.

a. Michigan's Whistleblowers' Protection Act (WPA), MCL 15.361 et seq.

i. The WPA prohibits employers from retaliating against employees who report violations of law, participate in investigations, or refuse to engage in illegal activities.

b. Federal statutes such as the Sarbanes-Oxley Act and the Dodd-Frank Act.

i. These federal statutes provide protections for employees in financial and corporate sectors who expose fraudulent or unlawful conduct.

2. Employers should create clear internal reporting mechanisms, provide assurances against retaliation, and ensure compliance with legal protections.

a. Establishing anonymous reporting options and fostering a culture where employees feel safe speaking up.