Report From Counsel — Spring 2023

Rudolph Friedmann LLP

ATTORNEYS AT LAW
617/723-7700 • www.rflawyers.com

Real Estate; Civil Litigation; Bankruptcy & Insolvency; Corporate & Partnership; Commercial Matters; Employment; Personal Injury; Construction; Business & Estate Planning; Divorce; Hotel & Restaurants; Patent & Intellectual Property; Criminal Defense

The End of An Era: The FTC Proposal to Ban Noncompete Agreements

by Casey Sack, Esq.

In a stunning proposal, the Federal Trade Commission (FTC) has proffered a universal ban on noncompete agreements. This proposal, albeit a considerable step away from the norm, was not necessarily unpredictable. Most recently, the FTC made a preliminary finding that noncompete agreements constitute an unfair method of competition and therefore violate Section 5 of the Federal Trade Commission Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." If this proposal is enacted, it would have sweeping consequences in Massachusetts.

What is a Noncompete Agreement?

A noncompete agreement is precisely as it sounds. A noncompete agreement or noncompete clause is a contractual agreement or provision between an employer and a worker that bars the worker from working for a competing employer or starting a competing business. Noncompete agreements are typically within a certain geographic area and for a limited period of time after the worker's employment ends.

Noncompete agreements have long been a source of controversy. The agreements tend to be a reliable scapegoat for stagnating the pay of middle-income workers, preventing such workers from switching jobs to secure a raise.

However, noncompete agreements are not necessarily perceived as all bad. These agreements protect established companies by limiting competition within industries to allow those companies to thrive and protect the products it sells to consumers.

Scope of the Proposal

The scope of the FTC's proposal is quite expansive. Applicable to both employees and independent contractors, the FTC would require employers to withdraw existing noncompete agreements and to inform workers that they no longer apply. Likewise, employers would be precluded from entering into, attempting to enter into, and maintaining a noncompete agreement with a worker. Also, employers would not be able to imply that a worker is bound by a noncompete agreement when he or she is not.

For existing noncompete agreements, which cover a considerable portion of workers in the private sector, the proposal would require employers to affirmatively rescind existing noncompete agreements and notify workers that they are no longer subject to the agreement's terms.

The proposed rule does provide for certain exceptions. If the proposed rule is enacted, an anticipated formidable exception is the sale-of-business exception for an owner, member, or partner who owns at least twenty-five percent of a business that is being sold. Specifically, the exemption also covers those who are "otherwise disposing of all of the person's ownership interest in the business entity, or by a person who is selling all or substantially all of a business entity's operating assets, when the person restricted by the non-compete clause is a substantial owner of, or substantial

(continued on page 2)

The End of An Era: The FTC Proposal to Ban Noncompete Agreements

(continued from page 1)

member or substantial partner in, the business entity at the time the person enters into the non-compete clause."

The proposal is likely to be enacted in some form, though the scope of the enactment is difficult to predict. As such, it makes sense to assume that existing noncompete agreements will be affected by this proposal. If you need help reviewing your noncompete agreement or discussing these proposed changes, contact the Rudolph Friedmann attorneys at (617) 723-7700.

Who Bears the Burden for a Fraudulently Intercepted ACH Payment?

by Sean B. Cullen, Esq.

Imagine you receive an email from a known creditor containing an invoice for an account payable. The email contains instructions for you to pay the invoice through an accredited clearing house ("ACH"). The email further contains the creditor's bank account information for depositing the ACH payment. You pay the invoice by depositing the ACH payment as instructed in the email. You later discover the creditor's email system was hacked and the bank account information provided in the email belonged to third-party hackers. The creditor never received the ACH payment and has not been compensated for the goods or services it provided you. Do you still owe the creditor? The law is still unclear. However, a recent decision on a preliminary motion by a federal judge of the United States District Court for the District of Massachusetts would indicate that, under certain circumstances, the answer may be yes. The decision sheds new light on the obligations of both purchasers and sellers when payment is made through an ACH.

Whether a purchaser is justified or excused from paying a seller due to a fraudulently intercepted ACH payment will ultimately depend on:

- Whether the seller took reasonable steps to secure or maintain its email system;
- Whether the seller knew, or should have known, that its email system had been compromised;
- Whether the purchaser took reasonable steps to verify the bank account information before attempting to pay the seller; and
- Whether the seller knew or should have known that the email and correspondence was fraudulent.

The case involved a breach of contract lawsuit for the sale of eggs. At the beginning of the parties' contractual relationship, the seller required the purchaser to enter into an ACH Agreement that provided the terms under which the purchaser would pay the seller for the eggs. The ACH Agreement specified the bank account belonging to the seller and authorized the purchaser to make deposits into that account for payment of the seller's invoices.

The parties' contractual relationship was at first uneventful. The seller delivered eggs to the purchaser, and the purchaser paid the seller for the eggs pursuant to the terms of the ACH Agreement. Roughly one-year into the parties' contractual relationship, however, the purchaser received an email that appeared to be from the seller's email account stating that the seller's bank account was changing and that the purchaser would receive new ACH payment instructions. Notably, the correspondence attached to the new ACH payment instructions incorrectly identified the seller's address, contained at least one additional typographical error, and was not personally addressed or signed.

The purchaser did not require a new ACH Agreement and did not follow up with a telephone call to the seller to verify the bank account in the new ACH payment instructions. For the next three months, the purchaser made nine deposits totaling almost one million dollars into the new bank account, completely unaware that this account was in fact controlled by third-party hackers, not the seller. The purchaser became aware of the fraud only after the seller made demand upon the delinquent account.

(continued on page 3)