SPECIAL ADVERTISING FEATURE TO COLUMBUS BUSINESS FIRST

COLUMBUS BAR ASSOCIATION

Legal Connections

CBA www.cbalaw.org

LEGAL EXPERTISE FOR THE BUSINESS COMMUNITY

AUGUST 20-26, 2021

Need a background check? The Columbus Bar provides BCI Background Checks at a convenient downtown location. Schedule an appointment Monday through Friday: www.cbalaw.org

Jill Snitcher McQuain, Esq.
Executive Director
jill@cbalaw.org

FTC LIMITS: UNDERSTANDING NON-COMPETE AGREEMENTS AFTER PRESIDENT'S EXECUTIVE ORDER

BY CHRISTOPHER TACKETT, ESQ.
Roetzel & Andress, LPA

As you have likely heard in the news, on July 9, President Biden issued an Executive Order on "Promoting Competition in the American Economy." The Order directs the Federal Trade Commission to develop proposed rules that would purport to limit enforceability of certain non-compete agreements. It is part of a larger initiative by the Biden Administration to promote competition in the American economy and allegedly remove barriers to economic growth.

Because the Order has been highly publicized, it has created confusion among business owners and high-level employees who are parties to non-compete agreements. There has been much debate about whether a widespread limit on non-competes will truly help businesses. In the spirit of clearing up some of this confusion, below are some key takeaways about the Order and the status of non-compete law.

1. The Law on Non-compete Agreements Has Not Changed.
President Biden's order does not create any change regarding the law governing your non-compete agreements. Rather, the Order simply directs the FTC to make a proposed federal rule placing limits on non-competes. But, the agency's rulemaking process can take months or even years. There is also a question of whether the FTC has authority to regulate this area of law through rulemaking. A sweeping federal rule would be a significant departure from historical treatment of this area and will be tied up in court challenges even upon approval of a rule.

2. A Federal Rule Attempting a Complete Ban on Non-compete Agreements is Unlikely.
It is presently unclear what level of regulation the FTC will attempt. But, it does not appear that the FTC will issue a complete ban on non-compete agreements. Many businesses and unfair competition lawyers, like myself, consider non-competes to be essential for employees who possess trade secrets and confidential information. This is for good reason; a study from the Ponemon Institute and Symantec Corporation showed that "59 percent of ex-employees admit to stealing confidential company information" when they leave their job. The harm caused by this loss can be substantial. Thus, when used appropriately, noncompetition agreements can be an extremely effective tool to prevent the harm caused by this type of information removal.

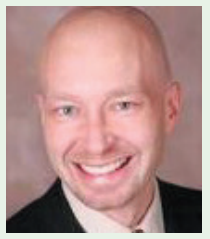
Instead, the FTC may take a narrow approach by banning non-compete agreements for low-wage workers rather than for everyone. Several states have already done so, because these workers typically have less ability to move outside the geographic area specified in the non-compete.

3. Many Believe that the FTC Does Not Have Authority to Regulate Non-Compete Agreements.
The enforcement or limitation of non-compete agreements has always been regulated by the individual states throughout the history of American law, and there is no precedent to support the FTC regulating non-competes. Each state has its own laws about the agreements, and these laws vary widely by state. Three states (California, North Dakota and Oklahoma) have banned employee noncompete agreements altogether. A dozen other states prohibit them with low-wage workers. Most states, including Ohio, enforce agreements that are tied to protection of a legitimate business interest and reasonable in time, scope, and geography.

Non-compete agreements are subject to the laws of individual states until the FTC issues new federal rules. Even in states where they are legal, however, courts may refuse to enforce non-compete agreements that are overly broad. For this reason, it is important for businesses to ask their legal counsel to review the agreements and ensure they comply with state law.

IT'S THE 10TH ANNIVERSARY OF OUR LEGAL PRACTICE LAB! JOIN US FOR THIS YEAR'S STELLAR SERIES: WWW.CBALAW.ORG

SUMMER CYBERSECURITY CHECKUP: WHAT EVERY ORGANIZATION SHOULD BE DOING THIS SUMMER



BY: PAUL UNGER, ESQ.,
Affinity Consulting Group

The flurry of ransomware attacks this year should be a reminder that none of us are safe and we should be doing more. Here are some items to add to your next leadership meeting.

1.Write/Update your Written Information Security Program (WISP).
In many states, such as Ohio (which was the first state to adopt such a law), having a WISP that "reasonably conforms" to one of the national data security frameworks provides organizations with some protections from negligence actions in the event of a data breach.

Just as important as providing businesses protection, having such a program and protocols in place will make everyone's data much safer. Your WISP should address the following security areas:

- **Designating employees responsible for the security program (a task force or committee)**
- **Identifying and assessing security risks**
- **Developing policies for the storage, access and transportation of personal information**
- **Imposing disciplinary measures for violations of the WISP**
- **Limiting access by or to terminated employees**
- **Overseeing the security practices of third-party vendors as well as contractors**
- **Restricting physical and digital access to records**
- **Monitoring and then reviewing the scope and effectiveness of the WISP**
- **Documenting data security incidents and responses**

2. Mandatory Quarterly Training for Everyone.
Schedule mandatory education at least every quarter for everyone in your organization. Cybersecurity practices and education is not a one-time event. Your organization should be regularly revising your WISP and educating your people even more. Most successful cybercrimes involve human error. Talk to your IT folks about implementing a ransomware education and testing solution.

3.Multi-Factor Authentication Solution.
Implementing two-factor (or multi-factor) authentication (also known as 2FA or MFA) is just as important, or arguably more important, than changing passwords or using unique passwords. MFA is important because even if a cybercriminal has your username and password, without the second measure of authentication (usually using a tool like Google or Microsoft Authenticator, a text message notification requiring your intervention, or providing your fingerprint from your smartphone) they will not be able to login to an important service or account.

Read all six tips now at www.cbalaw.org/news.