



Trade Secret Quarterly

Fall 2020

You're *Not* on Mute – Protecting Trade Secrets in a Remote World

Let's set the scene: You are running a few minutes late to an important Zoom meeting with a potential client. You hurriedly search for the dial-in information. Then, you type in the 10-digit meeting ID buried at the bottom of an email. Next, you enter your password. And now, you have been corralled into a virtual waiting room where you must stay in meeting purgatory until the host grants you access to the call. Is all this *really* necessary?

According to the Delaware Chancery Court – yes. And, for the sake of your trade secrets in the COVID era, it most certainly is.

In *Smash Franchise Partners, LLC v. Kanda Holdings, Inc.*, No. 2020-0302-JTL, 2020 Del. Ch. LEXIS 263 (Ch. Aug. 13, 2020), plaintiffs Smash Franchise Partners, LLC, and Smash My Trash, LLC (jointly, "Smash") failed in their effort to convince the Court of Chancery of Delaware to issue a preliminary injunction barring the defendants from using or disclosing Smash's confidential and proprietary information. They claimed trade secrets were disclosed during Zoom meetings between Smash and prospective franchisees. However, the Zoom calls helped doom plaintiff's request.

Smash operates a franchised mobile trash compaction business. Smash's program for recruiting prospective franchisees included numerous meetings with current Smash franchisees, as well as Smash's founder. As a result of the pandemic, these meetings were all held on Zoom. The defendant expressed interest in a Smash franchise and

engaged in the beginning stages of the franchising process with Smash, but soon concluded that he could create his own mobile trash compaction business. Despite deciding to form his own business, the defendant continued to feign interest in a Smash franchise and gather information about Smash before starting out on his own.

Smash brought claims for misappropriation of trade secrets, conversion, unfair competition, and breach of a non-disclosure agreement, based on allegations that the defendant stole trade secret information that he learned during the virtual franchisee meetings conducted via Zoom. The court, however, held that Smash was not reasonably likely to succeed on the merits of its misappropriation claim because, even assuming trade secrets existed, Smash failed to take reasonable measures to protect them. This was based on the court's finding that Smash failed to use security measures to protect its information. The court noted:

- Smash freely gave out the Zoom information for the Franchisee Forum Calls and the Founder Calls to anyone who had expressed interest in a franchise and completed the introductory call;
- Smash used the same Zoom meeting code for all its meetings;
- Smash did not require participants to enter a password and did not use the waiting room feature to screen participants;
- Anyone who had expressed interest and received the code could join the calls, and participants could readily share the code with others; and

- The record establishes that twenty participants who could not be identified listened to the meetings. There was no evidence that these individuals signed NDAs.

Because of these security shortcomings, the court found that Smash had not taken reasonable steps to protect its trade secrets.

Practical tip: Information is not a trade secret unless it is “the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” In the age of COVID-19, the metric of “reasonable efforts” embraces an expectation that employers will understand and utilize the various security features included with remote communications platforms. Employers should make certain that every person in their organization who uses remote communication platforms receives adequate security training.

The New Reality

The court’s decision in *Smash* underscores the renewed importance of security and confidentiality in the remote world brought on by the COVID-19 pandemic. Traditional best-practices and tactics utilized to protect trade secret information have not changed – employers should continue to take steps such as identifying trade secret information for employees, limiting access to those with a need to know, using passwords and secure log-ins, utilizing security software, and considering data encryption.

Still, with an increased number of employees who are continuing to work from home, employers must confront the fact that working remotely creates risks to the integrity of trade secrets – whether employees are properly trained or not. Noteworthy risks include:

- Increased hacking risks;
- Remote handling of trade secret documents and information;
- Cross mingling of personal devices and proprietary information;
- Inadvertent disclosure to household members or third parties;

- Less visibility over communications from employees to third parties; and
- Increased risk of phishing and spam.

Next Steps

The new remote work “normal” requires employers to take a fresh look at trade secret protection. Best practices could include:

- **Beefing up home security measures**, like requiring minimum home security metrics for employees’ home internet networks and multi-factor authentication to log into to a company portal;
- **Imposing restrictions on the use of portable devices**, like blocking USB ports or prohibiting the use of portable electronic devices;
- **Monitoring policies** for routine, suspicious use, and key data access;
- **Defining personal device policies** which require baseline security and virus protection, updates, utilize remote wiping technology, and prohibit the transfer of trade secret information; and
- **Training employees** who use video conferencing services such as Zoom to discuss sensitive topics to use the services’ security features.

FOR MORE INFORMATION

For more information, please contact:



Deborah S. Brenneman

513.352.6638

Deborah.Brenneman@ThompsonHine.com

Debbie represents management in all areas of employment law, with a focus on trade secret and non-compete cases. She has a wealth of experience in successfully litigating and resolving these matters in state and federal courts across the country.



Hannah E. Caldwell

216.566.5908

Hannah.Caldwell@ThompsonHine.com

Hannah is an associate in the firm's Labor & Employment practice group. She advises employers on a broad range of labor and employment issues, including discrimination, harassment, wrongful discharge, trade secrets and restrictive covenants.

This newsletter may be reproduced, in whole or in part, with the prior permission of Thompson Hine LLP and acknowledgement of its source and copyright. This publication is intended to inform clients about legal matters of current interest. It is not intended as legal advice. Readers should not act upon the information contained in it without professional counsel.

This document may be considered attorney advertising in some jurisdictions.

© 2020 THOMPSON HINE LLP. ALL RIGHTS RESERVED.