

**COVID-19 – PROTECTING
TRADE SECRETS WITH A
REMOTE WORKFORCE**
ARTICLE SERIES



AELEX

APRIL 2020

www.aelex.com

INTRODUCTION

The continuing spread of the coronavirus has led to different nations issuing directives to their nationals to stay indoors in order to contain the spread of the virus. For instance, in the United Kingdom, the Prime Minister issued various directives ordering UK residents to stay at home and also empowering the Police to break up public gatherings and fine residents that disobey the directives.[1] In the United States, over 316 million residents in about 42 states have been urged to stay at home and these numbers may still rise.[2]

African nations have also issued emergency orders with Nigeria and Ghana directing residents in some selected states to close their offices and stay at home for a period of time. For some nations, it is uncertain when offices will reopen and life will return to what many have considered as normal.

This situation has led to employees having to work from home (WFH). This immediately raises concerns for employers as they would have to take certain measures to ensure that any trade secrets or valuable information that their employees have in their possession are kept confidential during this period and thereafter.



WHAT IS A TRADE SECRET?

A trade secret is defined as “a formula, process, device, or other business information that is kept confidential to maintain an advantage over competitors; information includes a formula, pattern, compilation, program, device, method, technique, or process.”[3]

The inference drawn from the above legal definition is that any confidential business information which provides an enterprise a competitive edge may be considered a trade secret and is an intellectual property right.

[1] Rob Picheta, 'Boris Johnson issues stay-at-home order, sending UK into lockdown to fight coronavirus pandemic' (cnn.com, 23 March 2020). <<https://edition.cnn.com/2020/03/23/uk/uk-coronavirus-lockdown-gbr-intl/index.html>> Accessed on 12th April 2020.

[2] Sarah Mervosh, 'See Which States and Cities Have Told Residents to Stay at Home'. (New York Times, 7 April, 2020) <<https://www.nytimes.com/interactive/2020/us/coronavirus-stay-at-home-order.html>> Accessed on 12th April 2020

[3] Black's Law Dictionary, 11th Edition

Although different countries have legislation that provides for the protection of trade secrets (for example in the US, there is the Uniform Trade Secrets Act) Nigeria does not have any existing legislation. Trade secrets in Nigeria are therefore protected under contract, tort and other basic legal principles.

The factors that qualify confidential information as trade secrets^[4] are:

- a) It is a secret not generally known to the public;
- b) It must have commercial value; and
- c) It has been subject to reasonable steps, by the person lawfully in control of the information, to keep it secret.

The implication of the foregoing is that the moment a trade secret becomes public knowledge, it loses its protection and this could affect the company's revenue, particularly when the company's business

edge is derived from the value of the trade secret. For example, The Coca-Cola Company's multibillion dollar business is premised on the trade secret for its secret Coca-Cola formula. It is likely that if that trade secret is made public, other competitors will be able to use this information to their advantage and The Coca-Cola Company could lose its market edge.

Additionally, businesses usually have obligations of confidentiality to their customers and business partners under contracts or non-disclosure agreements. Many of these agreements will require compliance with strict obligations that must be observed. Thus, the failure to take appropriate steps to safeguard the confidential information of another business could lead to a potential lawsuit.

WFH therefore presents a dilemma to the employers as they must put parameters in place to ensure that even though they grant employees access to trade secrets, sufficient measures are taken to keep the secrets protected. Additional measures are also necessary for circumstances where the employees are disengaged from the company. Risk of exposure can come from many sources, including lost or misplaced documents or devices and persons who may hack into the employee's devices or cloud storage system. In addition, the employee's personal devices may have less security or may be linked to other devices thereby making vital information prone to leakages.

PRACTICAL STEPS TO ADOPT TO PROTECT TRADE SECRETS

There is no single approach to protecting against the disclosure of trade secrets and each company is expected to assess the risks of misappropriation and adopt practical steps that can reasonably protect its information. Consequently, some of the practical steps that can be taken by the company to safeguard trade secrets include the following:

- + **Companies should ensure that their employees' contracts of employment contain non-disclosure and non-compete clauses that prohibits the employees from disclosing or compromising trade secrets where the employees are disengaged from the company. Furthermore, at the point of their disengagement, the company should remind them of their continuing obligation of confidentiality.**



- ✦ Companies should have policies in place that provide how trade secrets are to be handled and protected when employees are working remotely. These policies should also have confidentiality and non-disclosure clauses for employees who are to have remote access to trade secrets.
- ✦ Employers should educate employees on how crucial trade secrets are to the companies' business. They should also be able to identify the information that is regarded as trade secrets and keep them confidential at all times. Where possible, periodic reminders should be sent to employees reiterating that access to the trade secrets is restricted to only persons who have a legitimate need to have the information.
- ✦ Cybersecurity policies must be updated to address the unique risks of WFH. The company may have to direct its employees not to use personal devices when working on official documents as there remains the possibility that such personal devices may be hacked or have existing malware.

The company may also have to invest in anti-virus and software that would be able to identify when there has been any hack into any of its employee's devices so that steps can be taken to disable its network.

- ✦ Employers should provide protection when accessing confidential information by utilising two-step or multifactor authentication features. Employees who are working remotely and using personal or home WiFi should also secure those points of access with passwords.
- ✦ A departing employee's login credentials to the company's systems, including mobile phone access and video conferencing software, should be de-authorized. He or she should also be removed from the company's email distribution lists to avoid video or audio conference meeting invitations being sent to inappropriate individuals.



- + Employees should be constantly reminded about the proliferation of malware, phishing emails, social engineering and other scams. Employees who have access to proprietary or trade secret information should take reasonable steps to confirm the identity of anyone with whom they may be electronically communicating about proprietary or trade secret information, before transmitting any such information.**
- + Confidential information should be treated carefully and should not be printed and placed carelessly. However, if materials must be printed, they should be safeguarded and not just disposed of in a refuse bin. They must be destroyed or put through a shredding machine.**

CONCLUSION

Protection of trade secrets remain paramount during these times and even though the steps identified in this article are not exhaustive, having them in place could safeguard confidential information during this WFH period and even after employees resume work at their offices.





Davidson Oturu
PARTNER

AELEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana. A profile of our firm can be viewed [here](#). You can also visit our website at www.aelex.com to learn more about our firm and its services.'

COPYRIGHT: All rights reserved. No part of the publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means without the prior permission in writing of AELEX or as expressly permitted by law.

DISCLAIMER: This publication is not intended to provide legal advice but to provide information on the matter covered in the publication. No reader should act on the matters covered in this publication without first seeking specific legal advice.

Contact us at:

4th Floor, Marble House,
1 Kingsway Road, Falomo Ikoyi,
Lagos, Nigeria

Telephone: (+234-1) 4617321-3, 2793367-8, 7406533,

E-mail: lagos@aelex.com

Click here www.aelex.com

to follow our social media handles click below

    @aelexpartners