

Safeguarding an employer's trade secret: Insights from a Landmark Legal Case in Uganda.

In the ever-evolving landscape of employment law, new frontiers continually emerge, posing dilemmas for employees and employers alike, especially in cross-border contexts. With the advent of the digital age, where company data is integral to business operations, instances of employees misappropriating such data upon leaving employment have become increasingly common. This presents significant challenges in addressing such breaches, particularly for employers with operations spanning multiple jurisdictions. Further, the transient nature of digital assets adds another layer of complexity, as they can easily be deleted, destroyed, or exploited inappropriately. What recourse, then, should an employer have in such situations?

A recent case before the High Court of Uganda, Nile Breweries Limited v. Johnson Sebuggwawo; High Court Misc. Application No. 252 of 2024 sheds light on this issue. Johnson, formerly employed by Nile Breweries Limited ("Nile Breweries") from March 26, 2012, to April 4, 2023, resigned from his position as a trade marketing executive. Shortly thereafter, he joined Uganda Breweries Limited, the competitor of Nile Breweries, as a trade marketing executive.

Upon suspicion of misconduct, Nile Breweries took immediate action and initiated investigations into Johnson's activities prior to his departure from Nile Breweries. These investigations revealed that Johnson had transferred 125 emails from his official email address to his personal email address, comprising confidential company information without authorization. Nile Breweries, recognizing the seriousness of the breach, filed a case against Johnson for breach of his employment contract and unauthorized disclosure of trade secrets.

As the case remains pending in court, Nile Breweries took further steps to protect their trade secrets. They sought interim relief through an application for Anton Piller orders. These orders, if granted, would allow the inspection of Johnson's residence and the seizure of all computers, documents, materials, and articles found therein relating to the Nile Breweries's trade secrets or business information. This is a significant legal measure that can be used when there is a reasonable fear that evidence of infringement of intellectual property rights, in this case, trade secrets, could be destroyed or lost if the defendant is alerted before the search.

The court granted the application, noting the gravity of the situation. The content of the emails sent to Johnson's personal address contained sensitive business information, including marketing strategies and statistics. Given Johnson's role as a trade marketing executive, the court found it implausible that his actions were innocent. It was deemed highly probable that he intended to utilize this information to the detriment of Nile Breweries.

Moreover, the court considered the potential harm Nile Breweries would suffer if it refused to issue the Anton Piller order. Without intervention, Johnson could continue to access, destroy, or replicate sensitive data, thus

exacerbating the damages. The court found that it was unlikely that in the 3 months leading up to his resignation, Johnson could innocently and without authorisation transfer Nile Breweries' sensitive business information from his work email address to his personal email address.

Thus, the issuance of the Anton Piller order was deemed necessary to safeguard Nile Breweries' interests and prevent further harm. The court, therefore, issued the Anton Piller injunction as prayed by Nile Breweries.

The Nile Breweries case does not stand in isolation around the commonwealth. In 2015, the Court of Appeal of Alberta upheld an Anton Piller Injunction in an almost similar matter in the case of *Peters & Co Limited v Ward*; 2015 ABCA 6. The genesis of this case was that Mr. Ward who was described in court documents a 'key and senior' employee took confidential information about active and inactive corporate transactions, client board-level advisory presentations and documents from his ex-employer, Peters & Co, before resigning and joining their competitor. He had equally downloaded an entire database of client contact information and contact lists.

This led Peters & Co to institute a claim against Ward. The lower court issued Anton Piller orders in an interim application by Peters & Co for the search of Mr. Ward's property and the seizure of the documents which the court granted. Mr. Ward filed an appeal against the order of the lower court. The appeal challenged the order's validity, citing non-disclosure and failure to meet the order's prerequisites. The court rejected the appeal and affirmed the order's justification. It concluded that Peters & Co. adequately disclosed information and established a strong prima facie case of breach of contract and fiduciary duties. The court also upheld the seriousness of the alleged damage and the risk of destruction of evidence, justifying the need for the order.

Mitigating Risks and Protecting Trade Secrets:

Employers can mitigate the risk of data misappropriation by ensuring that all employees, especially those with access to sensitive information, sign comprehensive confidentiality agreements. These agreements should clearly outline the types of information considered confidential, the obligations of employees to protect such information, and the consequences of breaches. In Johnson's case, his employment contract expressly enjoined him not to copy any information from Nile Breweries without authorization. The court found that the 125 emails sent to his personal email address appear to have replicated the information without authorization.

Regular training sessions on confidentiality policies and procedures can reinforce employees' understanding of their obligations and the importance of safeguarding company data. In Johnson's case, such training might have raised awareness of the consequences of his actions and deterred him from engaging in misconduct.

Cross-Border Considerations:

While the decision in the Nile Breweries' case is specific to Uganda, its implications extend to cross-border employers or companies grappling with similar dilemmas in the region, offering valuable insights and legal strategies for addressing employee misconduct and protecting intellectual property rights across multiple jurisdictions. Employers facing similar situations in other countries in the region can draw insights from the legal reasoning and principles applied in this case and consider exploring similar legal remedies available in other jurisdictions in the region to protect their trade secrets and confidential information from unauthorized disclosure or misuse by former employees.

For cross-border employers, it's crucial to tailor confidentiality agreements and training programs to comply with the legal requirements of each jurisdiction where they operate. This ensures that their intellectual property rights are adequately protected and enforceable across multiple jurisdictions. Additionally, cross-border employers should stay informed about legal developments related to intellectual property rights and employee misconduct in the countries where they operate. This proactive approach allows them to adapt their policies and procedures accordingly and minimize the risk of data breaches and unauthorized disclosures.

Should you have any questions regarding the information in this legal alert, please do not hesitate to contact [Faith Macharia](#) or [Ernest Sembatya](#).



Faith Macharia

Partner

ALN Kenya | Anjarwalla & Khanna Kenya

faith.macharia@aln.africa



Ernest Sembatya

Partner

ALN Uganda | MMAKS Advocates

sembatya@ug.aln.africa

Contributors

1. Edwina Warambo - Senior Associate, ALN Kenya | Anjarwalla & Khanna
2. Edel Ouma - Senior Associate, ALN Kenya | Anjarwalla & Khanna
3. Alex Samson Ntale - Principal Associate, ALN Uganda | MMAKS
4. Leah Muhia - Associate, ALN Kenya | Anjarwalla & Khanna
5. Kibet Brian - Trainee Lawyer, ALN Kenya | Anjarwalla & Khanna