Articles + Publications | October 12, 2023

A Tale of Two Startups: Intense Competition Leads to Attempted Corporate Espionage

WRITTEN BY

Evan Gibbs | William M. Taylor | Alison A. Grounds | Michael I. Frankel | Megan Conway Rahman | Tiffany N. Bracewell

A recent incident highlighted in a *New York Times* article involving two rival startups is raising eyebrows in the fiercely competitive world of artificial intelligence (AI) and beyond. This incident, summarized below, highlights the importance of both practical and legal precautions companies should be considering.

The Incident

According to the *Times* article, in April 2022, Arthur AI, a New York-based AI company, received a request for a Zoom demonstration of its technology from a startup called OneOneThree. The head of technology at OneOneThree, Yan Fung, expressed interest in purchasing Arthur AI's technology. But there were some immediate red flags.

First, prior to the Zoom meeting, Arthur AI employees recognized that OneOneThree had no website. The *Times* article says that Fung told Arthur AI at the time that OneOneThree was in "stealth mode," which is why it had no website. Then, when Arthur AI asked Fung to sign a nondisclosure agreement (NDA), he reportedly asked Arthur AI to "hold off on the NDA," and Arthur AI agreed.

Despite these issues, a Zoom meeting was arranged to demo the technology. Fung said Karina Patel, OneOneThree's "main engineer," would dial in to the meeting. However, during the Zoom meeting, an attendee logged in under the name of Aparna Dhinakaran, which an Arthur AI employee immediately recognized as a founder of Arize AI, a rival startup. When recognized, the attendee quickly logged off. Arthur AI later deduced that Fung was, in fact, an employee of Arize AI named Dat Ngo, and OneOneThree was an inactive company of his.

After the call concluded, one of Arthur AI's employees messaged Ngo via LinkedIn direct messaging. Ngo responded by trying to recruit the Arthur AI employee, according to the *Times* article.

Legal Issues and Preventative Measures

This incident highlights several legal and practical issues that companies need to be aware of. It should go without saying that using false identities to gain a competitive advantage can lead to serious legal repercussions, including claims of fraud, misrepresentation, and unfair competition, among others.

©2026 Troutman Pepper Locke

To prevent and mitigate attempts at corporate espionage like the one experienced by Arthur AI, companies should consider the following preventative measures:

1. **Require NDAs Every Time.** NDAs are crucial in protecting sensitive information, especially during demonstrations of or when sharing access to proprietary technology, data, or documents. In this case, Arthur AI asked Fung to sign an NDA, but then agreed to proceed without one when he asked them to "hold off on the NDA." Although there would likely still be legal recourse for a company on similar facts, NDAs provide important legal benefits otherwise not likely available (*e.g.*, a clear cause of action for breach, liquidated damages, forum selection, etc.).

2. **Perform Proper Due Diligence and Act Consistently With Your Findings.** Companies should conduct thorough due diligence before sharing sensitive information. This includes verifying the identity and legitimacy of the other party. If your diligence produces any red flags, trust your gut and consider advancing no further without appropriate assurances from the other party and/or safeguards in place.

3. **Only Use Secure Communication Channels and Restrict Recording.** Companies should use secure communication channels and restrict access to meetings where sensitive information is shared. Companies should also be sure that the means of communication restricts unauthorized recording or capture of information being disclosed. However, a Zoom meeting could be recorded by a phone or camera by an attendee without the speaker knowing. For sensitive corporate information, companies should consider in-person presentations to reduce the risk of potential recording. Businesses should also think about restricting recording of confidential meetings by employees, given that many employees eventually leave to join competitors.

4. **Train Employees on Spotting and Responding to Potential Threats.** Nonmanagerial and nonexecutive company employees are very often gatekeepers of critical proprietary data or other materials, but are nevertheless unaware of what suspicious activity looks like and what they should do in response. Making sure employees are well-versed in these areas is critical.

5. **Conduct a Prompt and Careful Investigation Into Suspected Activity.** If a company suspects that its proprietary information has been taken, copied, accessed without authorization, or otherwise improperly used, it should quickly engage appropriate vendors and attorneys to investigate the matter. Time is usually of the essence in these matters and waiting may negatively impact resolution. It is also critical to ensure documents, data, and other materials that may be relevant evidence are properly preserved for later use, while also being mindful of privacy concerns and potential disclosure obligations to regulators.

It's natural for companies to seek an edge — especially in highly competitive industries like AI development. Companies should therefore be prepared to respond to corporate espionage threats and events in order to reduce security risks and avoid losing valuable time when an incident occurs. Click here to learn more about Troutman Pepper's Corporate Espionage Response Team.

RELATED INDUSTRIES + PRACTICES

- Business Litigation
- Corporate Espionage Response Team

©2026 Troutman Pepper Locke

- Labor + Employment
- White Collar Litigation + Investigations
- eDiscovery + Data Management