



Fortescue 'seized personal details'

The Australian

July 13, 2024 Saturday

Australian Edition

Copyright 2024 Nationwide News Pty Limited All Rights Reserved

Section: BUSINESS; Pg. 28

Length: 736 words

Byline: Angelica Snowden, Nick Evans

Body

Fortescue seized personal banking details of former employees that were the subject of raids conducted by the mining giant - as well as the entire business records of rival green iron start-up -Element Zero - claims in the Federal Court show.

The "extraordinary" orders won by **Fortescue**'s lawyers include details of private negotiations between Element Zero and other **Fortescue** rivals, as well as deeply personal information of its staff, potentially including personal banking passwords and private communications between the former **Fortescue** staff and their families.

Documents released by the Federal Court on Friday also show that, despite **Fortescue**'s claims its former staff stole its intellectual property, the iron ore giant was last year selling its would-be rival iron ore to help them test their own technology, and had agreed to protocols for the exchange of information about how well it worked using **Fortescue** ore.

The new revelations come after **Fortescue** executive chairman Andrew Forrest claimed he did not know his company paid private investigators to follow the wives of his ex-staff Bart Kolodziejczyk and Bjorn Winther-Jensen into Kmart, take pictures of their children and rummage through mail before court-sanctioned raids were launched on their homes and offices. **Fortescue** won court orders to carry out raids in May after it was alleged Element Zero's Dr Kolodziejczyk, Dr Winther-Jensen and Michael Masterman stole **Fortescue**'s carbon-dioxide-free green iron tech-nology secrets when they all quit several years ago.

Despite elements of the court case remaining suppressed, fresh documents released on Friday revealed Element Zero's concern that an "extraordinarily large volume" of electronic material - more than three terabytes - belonging to its young business was captured during the searches.

Element Zero's Gilbert & Tobin lawyer Michael Williams said virtually the entirety of Element Zero's documents and emails were seized, "together with highly confidential and privileged material" that was "entirely unrelated to **Fortescue**'s pleaded claim". The entire contents of Dr Kolodziejczyk's mobile was downloaded, including photos and videos, and about 3TB of data was captured, which Mr Williams said was "an extremely large volume" to be caught under Anton Piller search orders in his experience.

Fortescue 'seized personal details'

Further, he said there were grounds for the search orders to be scrapped based on "the apparent extraordinary invasion of the privacy of the respondents".

"I am informed by Mr Masterman and believe that, as a result of how the search orders are drafted and executed they will have captured a very large amount of information that is confidential, privileged, and not likely to be relevant to these proceedings," Mr Williams said.

"The search orders will have captured material that is ... highly confidential to third parties including competitors of **Fortescue**." As well, Mr William said he believed images taken of Dr Kolodziejczyk's phone would have captured data including passwords for online banking and superannuation.

According to a summary of **Fortescue**'s arguments, staff became suspicious about the activities of the three men after they realised Mr Masterman was working with Dr Kolodziejczyk and Dr Winther-Jensen in September, that they incorporated Element Zero, which was "potentially developing technology that is similar to technology â€ developed for **Fortescue**", and that Element Zero was "seeking the supply of iron ore samples from **Fortescue** to help test (Element Zero's) technology".

A story published in the Australian Financial Review on January 17 kicked off their concerns.

"The AFR article set in train a line of inquiry at **Fortescue**, which involved reviewing the projects that Dr Kolodziejczyk and Dr Winther-Jensen had been working on, and investigating their **Fortescue** email inboxes, group SharePoint folder and two laptops on suspicion of IP leakage," the summary read.

After Dr Kolodziejczyk resigned in October 2021, he attended a meeting at which he was told he could not work at **Fortescue**'s office to finish his notice period. Dr Kolodziejczyk was told he could "make copies and use documents he needed" to wrap up and that he should delete "everything" saved locally on his **Fortescue** laptop before he returned it because the company had copies on SharePoint. He continued to work on patent applications for **Fortescue** up until he left the company, court documents said.

Load-Date: July 12, 2024