SUMMER 2022 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss data exfiltration including prevention, digital forensics and case law.

You Can't Take It with You: Pursuing Data Exfiltration Claims Against Former Employees

There's no question that data exfiltration can damage an organization in many ways. Whether it's lost sales revenue, damage to reputations, or something as drastic as stolen product designs, data exfiltration is worth preventing, and in the event of an occurrence, worth pursuing. With the Great Resignation bringing greater employee turnover, employers should wisely consider the legal implications of what needs to be done before and after employees walk out with proprietary information. Several recent cases highlight important considerations when pursuing in court data exfiltration by employees.

Policy Only Works When Followed

The wisdom of proactively setting policies regarding the use and misuse of organization data, equipment, tools, and Bring Your Own Device policies are championed by Human Resources executives and legal counsel. By now, if an organization doesn't have policies codified, published, and acknowledged, it should be prepared for some headshaking in the courtroom. However, as demonstrated in *DM TRANS, LLC d/b/a ARRIVE LOGISTICS v LINDSEY B. SCOTT; MATTHEW J. DUFFY; SCOTT C. MAYER; FRANK J. HERNANDEZ; BRYAN C. KLEPPERICH; JAKE HOFFMAN; and TRAFFIC TECH, INC.* (Case No. 21 C 3634. US Dist. Ct, N.D. Illinois, Eastern Division, 2021), if an organization doesn't follow up on its policies designed to prevent data exfiltration, some advantage may be lost. In this case, even though the defendants admitted during deposition that they had data belonging to their former employer on their personal devices, the plaintiff's inaction eroded the effectiveness of what might normally be a "gotcha!" As Judge Leinenweber wrote in his opinion:

> Because Arrive did not provide its own devices for employees to work from home, Defendant Employees were required to use their own devices to Arrive's benefit. Arrive then failed to ask any questions about the information remaining on

> Defendant Employees' personal devices and did not terminate access to Arrive's work email system. These failures are the responsibility of Arrive as part of its reasonable measures to secure its confidential information. For these reasons, the Court finds there to be a low probability that there are trade secrets, first because of the undeveloped record as to what the secrets are, and second because of the inconsistent record on Arrive's ability to keep reasonable care of its information.

Not only does the opinion fault the employer for not following its own policies with respect to protecting data, but the court also goes on to say, in essence, the data couldn't have been that important if they didn't protect it after employment termination, as they'd already secured a right to do in their employment agreements. This is a lesson for any organization, as it's a reminder that a plaintiff cannot pursue damages for the loss of property of which adequate care isn't taken.

Courts Reward Thorough Discovery

Not all data exfiltration cases rely on cellphones and laptops, and there is ample evidence that no stone should be left unturned when investigating data theft. Thanks to a well-executed and thorough discovery investigation, the plaintiff in *SFX INSTALLATION, INC. v. JERAL PIMENTEL and TRANSCENDENT BUILDERS CONSTRUCTION CORP.* (Civ. No. 21-cv-11326 US Dist. Ct, D. New Jersey, 2021) was able to prove that the defendant was working for his own company while on his employer's time, using his employer's vehicle and tools, and making sales calls to his employer's customers for his own benefit. The judge points to a number of items that a thorough discovery confirmed were misappropriated:

> Additionally, the entrustment of the company's employees, vehicle, EZ-Pass card, phone, and tools to Pimentel suggest that he occupied a position of "trust and confidence" within SFX, which he breached by using the company's resources for solicitation and other work for Transcendent…
>
> …Thus, the Court finds that SFX has asserted facts to demonstrate that it suffered irreparable injury when Transcendent took its customers, and still suffers irreparable injury because Transcendent continues to solicit and work for former SFX customers, and employ former SFX employees.

Interestingly, the Court gave the defendant some leeway with his claim that following his resignation, he didn't seek to access his former employer's VPN despite still having the ability to do so. The judge does not indicate whether there was any eye rolling, winking, or nodding in response.

Be Sure to Ask for What's Important

A carefully crafted motion can cut down on the effort required to get court-ordered protection against data exfiltration. If what you want is third-party verification from a trusted digital forensics provider that employer-owned data has been removed from a former employee's devices, the words chosen can make all the difference. In the Background section of Judge David C. Joseph's Memorandum Ruling in *VOLT POWER, LLC, v JAMES ERIC DEVILLE, ET AL.* (Civil Docket No. 1:21-CV-00395. US Dist. Ct, W.D. Louisiana, Alexandria Division, 2022), the judge records how a forensic discovery order led to an amended complaint:

> Generally, the Injunction: (i) prohibited Deville, and any third party with whom he had shared Volt Power's confidential and proprietary information or with whom he

> acted in concert with, from possessing Volt Power's proprietary information, and (ii) ordered that such information be purged from all electronic devices and databases and returned to Volt Power. [Doc. 37 p. 8]. The Court also ordered Volt Power and Shelton Energy to agree on a third-party forensic analyst to search Shelton Energy's electronic databases and any computers Deville used as an employee of Shelton Energy. [Doc. 37 p. 8].
>
> After the forensic examination was conducted, Volt Power filed an Amended Complaint adding Shelton Energy as a defendant and alleging that the forensic examination had revealed that Deville, "as a Shelton Energy employee, and presumably at Shelton Energy's direction," obtained Volt Power's information from his former colleagues to use at Shelton Energy. [Doc. 50 ¶ 9].

The benefit to the plaintiff/former employer in the case was that it not only had the opportunity to search the former employee's devices, but it was also able to force the removal of employer-owned information and confirmed the information was misappropriated. The good news would continue, as Judge Joseph denied the defendant's motion to dismiss in part because the plaintiff had so fully detailed his claims in previous filings, such as the Injunction referenced above.

The courts aren't always as impressed with well-worded pleadings as Judge Joseph was, but it's worth the extra effort to make sure that if you must take your case to court, you've got your i's dotted and your t's crossed. When it comes to preventing data exfiltration, you'll want to make sure that you follow policy, conduct diligent discovery, and make sure you have all the information you need to get back what's rightfully yours.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

BLACK HAT USA 2022
Las Vegas, NV: August 6-11, 2022

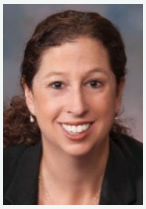
DEFCON
Las Vegas, NV: August 11-14, 2022

ILTACON 2022
National Harbor, MD: August 21-25, 2022

PFIC 2022
Nashville, TN: September 6-9, 2022

SEDONA CONFERENCE WG12 ANNUAL MEETING 2022
Reston, VA: September 7-8, 2022

Click here to see more upcoming events and links.



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: