



Internal Investigations ♦ Trade Secrets ♦ Employment Litigation

[SAMPLE ONLY*]

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

XYZ GROUP, INC.,
an Illinois corporation,
Plaintiff,
v.
SUSAN CURRIER,
an individual,
Defendant.
Case No.: 10 CV 4815
Judge John D. Smith

PLAINTIFF’S MOTION TO COMPEL DEFENDANT’S
PRODUCTION OF LAPTOP COMPUTER AND USB DEVICES

NOW COMES the Plaintiff, XYZ GROUP, INC. (“XYZ”), and moves this Court pursuant to Federal Rule of Civil Procedure 37(a) to enter an order compelling Defendant Susan Currier to produce her laptop computer and any external “USB” hard drives or flash (“thumb”) drives used by her in connection with XYZ business, as requested in XYZ’s Requests for Production No. 3 and No. 4.1 In support of its motion, XYZ states as follows:

1 See EXHIBIT A for common sources of electronic evidence.

* DISCLAIMER: This document is intended to be used as an example of a motion to compel discovery of electronically stored information. It is not intended to represent legal advice. This document contains fictional data. Any similarity to actual events or persons is purely coincidental.



Internal Investigations ♦ Trade Secrets ♦ Employment Litigation

1. On July 7, 2009, XYZ filed a Complaint for Injunctive and Other Relief, alleging violation of the Illinois Trade Secrets Act, the Computer Fraud and Abuse Act, and a breach of Defendant's employment contract.²

2. This matter stems from Defendant's inappropriate conduct which included, among other acts, the intentional stealing of XYZ's confidential engineering plans for products currently in development.

3. On March 5, 2009, Defendant was dismissed from her employment at XYZ as Lead Engineer. Shortly after her departure, XYZ computer technicians examined Defendant's work computer, used by her on a daily basis during her seven years of employment at XYZ. The technicians discovered a complete lack of user-specific files that should have been present on Defendant's computer due to normal use. This lack of files suggests that someone intentionally deleted files relating to Defendant's user profile.

4. The technicians also discovered a record, or "log file," of files accessed on XYZ computer servers from Defendant's work computer. This record showed that, on February 4, the day before Defendant's termination, the computer was used to access and copy forty-seven (47) files containing engineering diagrams of XYZ products currently in development. This action was beyond Defendant's authorized use of XYZ computer systems. Defendant would normally not copy plans to her local machine but would rather work on copies maintained on XYZ computer servers.

² The conduct of a terminated employee may constitute claims under state and federal law, including misappropriation of trade secrets, unauthorized access to computer systems, and breach of contract for violation of a non-disclosure agreement, non-solicitation clause, or covenant not to compete.

5. Forensic examination of Defendant's work computer produced a list of three USB devices that had been connected to the computer during Defendant's last two weeks of employment. XYZ believes these devices are thumb drives currently in Defendant's possession, custody, or control. One of these devices, labeled "Sammy" and with a serial number of 0000183D8774B645&1, was last accessed twelve (12) minutes after the copying of engineering files described above.

6. This information led XYZ to believe that Defendant had copied XYZ's confidential engineering plans from XYZ computer servers to her work computer, transferred these to the "Sammy" USB drive, and then attempted to delete all evidence of her actions from the work computer.³

7. XYZ served Defendant with Requests for Production on August 22, 2009. Request for Production No. 3 requested production of "Any and all USB devices, including external hard drives and flash ("thumb") drives, used on XYZ Group premises and currently in your possession, custody, or control." Request for Production No. 4 requested production of "Defendant's laptop, known to be used for XYZ business on December 21 through December 24, 2008."

8. Defendant has continually refused to comply with either of these requests.

9. Defendant's continued noncompliance has seriously prejudiced XYZ ability to go forward with this action. Defendant's possession of any of the three USB devices connected to her XYZ work computer will show Defendant's ability to steal XYZ trade secrets. Examination

³ It may be beneficial to clearly explain how the party has arrived at its conclusions based upon the technical and sometimes confusing digital evidence.



Internal Investigations ♦ Trade Secrets ♦ Employment Litigation

of Defendant's laptop computer may produce further evidence showing that Defendant had subsequently connected these devices to her own computer. If the engineering documents are no longer contained on the "Sammy" thumb drive, examination of the laptop computer is likely to also show what XYZ trade secrets were on the USB devices or are currently on Defendant's computer. Without production of the thumb drives and Defendant's laptop, XYZ will not be able to demonstrate which and how many engineering plans Defendant stole.⁴

WHEREFORE Plaintiff XYZ GROUP, INC. respectfully requests that this Court grant its Motion to Compel and enter an Order requiring Defendant Susan Currier to produce on or before December 1, 2009, any USB devices used by her on XYZ premises and her laptop computer as requested by XYZ's Requests for Productions No. 3 and No. 4.

November 1, 2009

Respectfully submitted,

XYZ GROUP, INC.

By: /s/ James R. Sheffield
One of Its Attorneys

James R. Sheffield
HILL, KLIMER, & SHEFFIELD
179 North Knox Street, Suite 1700
Chicago, Illinois 60603
(312) 999-0102

⁴ It is vital that the Motion to Compel clearly explain why the party seeks the production requested. Without such explanation, the Court may not understand the importance of a particular piece of digital evidence to the claims or defenses at issue and could not, therefore, properly weigh the benefits against the burdens of that production.



Internal Investigations ♦ Trade Secrets ♦ Employment Litigation

EXHIBIT A

POTENTIAL SOURCES OF ELECTRONIC EVIDENCE

When an employee leaves a place of employment, he may seek to take company data with him in a variety of forms. The following is a list of sources you may consider searching for valuable evidence of misappropriation.

1. Employer-issued laptop or desktop computers still in employee's possession, custody, or control
2. Employee-owned laptop or desktop computers
3. Computer hard drives previously used in relevant computer systems
4. Copies of hard drives or other computer equipment used by employee, when the original sources are unavailable
5. Corporate email accounts
6. Personal email accounts
7. Email attachments
8. Diskettes, CDs, DVDs, and other removable media
9. External (USB, FireWire) hard drives
10. Flash or "thumb" drives
11. Mobile devices, including cell phones, smart phones, PDAs, and BlackBerrys