



Internal Investigations ♦ Trade Secrets ♦ Employment Litigation

[SAMPLE ONLY¹]

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 FOR SANCTIONS DUE TO
DEFENDANT’S WILLFUL SPOILIATION OF EVIDENCE

NOW COMES the Plaintiff, XYZ GROUP, INC. (“XYZ”), and moves this Court pursuant to Federal Rule of Civil Procedure 37(b) and this Court’s inherent power to enter an order granting default judgment against Defendant Susan Carrier as sanction for willful spoliation of evidence contained on her laptop computer and “USB” flash drive. In the alternative, XYZ moves this Court for an adverse jury instruction preventing Defendant from arguing that her laptop computer did not contain XYZ engineering files. In support of its motion, XYZ states as follows:

1 DISCLAIMER: This document is intended to be used as an example of a motion for sanctions due to spoliation 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.

© 2011 Forensicon, Inc. For use as a template only. All other rights reserved.



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. 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.

2. 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 and 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.

3. 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 March 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.

4. 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. 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.

5. 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.

6. On November 1, 2009, XYZ moved this Court to enter an order compelling Defendant to produce her laptop computer and all USB drives in her possession used on XYZ business for forensic examination by XYZ’s computer expert. This Court entered the requested order on November 9.

7. On November 24, XYZ received Defendant’s laptop computer and three USB devices, including the drive labeled “Sammy.” XYZ’s computer expert immediately created forensic “mirror” images of the computer and USB devices and began a forensic examination of each. The resultant Expert Report is attached hereto as Exhibit A.²

8. Upon examination of the laptop computer, XYZ’s computer expert discovered several relevant files in slack space. Slack space is the area on a hard drive that has not be reallocated after a file has been deleted. This space often contains fragments of previously deleted files. The slack space on Defendant’s laptop contained four files known as xyzeg_0021.dwg, xyzeg_0094.dwg, xyzeg_1070.dwg and xyzeg_3906.dwg. These filenames match exactly to four engineering drawings currently saved on XYZ computer servers. These files were deleted from Defendant’s laptop on November 8, seven days after XYZ’s motion to compel production and only one day before this Court’s order of the same. Because they have been partially deleted, however, no further information relating to these files can be collected. Based on the

² An Expert Report should explain what the forensic analysis found, what the expert believes this data means for the parties involved, and how the expert reached his or her conclusions. It should be clear and thorough and may include information about the forensic tools and settings used in the analysis.



Internal Investigations ♦ Trade Secrets ♦ Employment Litigation

above, XYZ believes these files are four of the numerous XYZ proprietary engineering drawings Defendant took from XYZ's computer servers.

9. Examination of the "Sammy" USB drive showed that a one (1) had been written to every bit, a pattern consistent with the intentional deletion of data. Such a pattern is indicative of the use of a "scrubbing" or "wiping" program intended to permanently delete all data on the device. This pattern would not occur due to normal use, through which the device would contain a more random distribution of ones and zeroes. Examination of the remaining two USB devices produced no relevant data.

10. Both the Federal Rules of Civil Procedure and this Court's inherent power allow sanctions to be issued when a party destroys evidence that it could reasonably foresee would be relevant to litigation. *Jones v. Bremen High Sch. Dist.* 228, No. 08-C-3548, 2010 U.S. Dist. LEXIS 51312, at *14 (N.D. Ill. May 25, 2010). Appropriate sanctions for spoliation of evidence may include the issuing of a default judgment or an adverse jury instruction against the spoliating party. *Bryant v. Gardner*, 587 F. Supp. 2d 951, 958 (N.D. Ill. 2008); Fed. R. Civ. P. 37(b)(2). Default judgment may be entered against a spoliating party when there is "clear and convincing evidence of willfulness, bad faith or fault by the noncomplying party." *Krumwiede v. Brighton Assocs.*, No. 05-C-3003, 2006 U.S. Dist. LEXIS 31669, at *25 (N.D. Ill. May 8, 2006). A party's bad faith may be shown by that party's intent to hide unfavorable information. *Jones*, 2010 U.S. Dist. LEXIS 51312, at *17.

11. The evidence collected by forensic examination of Defendant's computer and USB device demonstrates that Defendant's actions warrant default judgment in favor of XYZ. Defendant's duty to preserve evidence began at least as early as XYZ's filing of the complaint



Internal Investigations ♦ Trade Secrets ♦ Employment Litigation

against her on July 7, 2009 and remained effective during November when the deletion occurred. Nevertheless, Defendant intentionally deleted files from her laptop computer and wiped the “Sammy” USB device in an concerted effort to hide this data from XYZ and this Court. Defendant’s willful spoliation of evidence seriously prejudices XYZ’s ability to go forward with this action by eliminating the clear and convincing evidence of Defendant’s recent possession of confidential XYZ engineering plans.

12. If this Court does not enter default judgment, this Court should impose a jury instruction adverse to Defendant, preventing her from arguing that her laptop computer did not contain confidential XYZ engineering plans. Such an argument has been conclusively proven false by the file fragments found on Defendant’s computer, which could not have appeared there if the files were not first copied to the computer.

WHEREFORE Plaintiff XYZ GROUP, INC. respectfully requests that this Court grant its Motion for Sanctions and enter default judgment in favor of XYZ, an adverse jury instruction preventing Defendant from arguing she did not have XYZ engineering plans on her personal laptop computer, or further appropriate relief.

January 12, 2010

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