**[Cite as *State v. D.S.*, 2008-Ohio-1950.]**

# COURT OF APPEALS OF OHIO

## EIGHTH APPELLATE DISTRICT
## COUNTY OF CUYAHOGA

STATE OF OHIO, :

Plaintiff-Appellee, :

No. 89844

v. :

D.S., :

Defendant-Appellant. :

---

JOURNAL ENTRY AND OPINION

**JUDGMENT:** AFFIRMED
**RELEASED AND JOURNALIZED:** April 24, 2008

---

Criminal Appeal from the Cuyahoga County Court of Common Pleas
Case No. CR-479157

---

***Appearances:***

William D. Mason, Cuyahoga County Prosecuting Attorney, and Robert Botnick, Assistant Prosecuting Attorney, *for appellee*.

Robert Tobik, Cuyahoga County Public Defender, and David M. King, Assistant Public Defender, *for appellant*.

PATRICIA ANN BLACKMON, J.:

**{¶ 1}** Appellant D.S. appeals her conviction for unauthorized use of a computer. She assigns the following errors for our review:

> I. Defendant's convictions on three counts of unauthorized use of a computer were not supported by sufficient evidence as required by due process in violation of the U.S. Constitution Amendment XIV and Crim.R. 29.
>
> II. Defendant's convictions for unauthorized use of computer were against the manifest weight of the evidence.
>
> III. The court erred by admitting state exhibits 1 through 4 under the business records exception to the hearsay rule in violation of the Evid.R. 801 and 802.
>
> IV. The court erred by admitting State's Exhibits 1 through 4 in violation of Evid.R. 1001.
>
> V. The court erred and denied the defendant due process under Ohio Constitution Article 1 Section 10 and U.S. Constitution Amendment V and XIV when it admitted State's Exhibits 1 through 4 in violation of Criminal Rule 16.

**{¶ 2}** Having reviewed the record and pertinent law, we affirm D.S.'s conviction. The apposite facts follow.

**{¶ 3}** On April 6, 2006, the Cuyahoga County Grand Jury indicted D.S. for three counts each of telephone communications fraud and unauthorized use of a computer. On June 15, 2006, D.S. pled not guilty at her arraignment, and after several pre-trials, a jury trial commenced on March 2, 2007.

**{¶ 4}** At trial, Janice Allen, a former origination manager in the loan operations department of Deep Green Financial, ("Deep Green") testified that she was D.S.'s immediate supervisor. Allen testified that on August 9, 2005, D.S.

called off sick, and it became necessary for Allen to gain access to D.S.'s electronic mail ("e-mail") and voice mailbox to follow up on any pending communications with Deep Green's clients. Allen contacted her manager to get approval to access D.S.'s e-mail and voice mailbox accounts.

**{¶ 5}** Allen testified that she accessed D.S.'s email and voice mailbox utilizing a password provided by Deep Green's information technology ("IT") department. Allen testified that while reviewing D.S.'s e-mail account, she discovered an e-mail that had been sent on August 8, 2005 to an outside e-mail address known as truloxs@hotmail.com. Allen further testified that the e-mail had an attached Excel spreadsheet containing confidential information on sixty-four of Deep Green's clients. Allen testified that after discovering the e-mail, she reported it to her manager, Patricia Kelly.

**{¶ 6}** Patricia Kelly, former manager of the underwriting origination department at Deep Green, testified that on August 9, 2005, she spoke with D.S., who indicated that she was unable to report for work because she was ill. Kelly testified that she asked Allen to review D.S.'s workload, and Kelly arranged with the IT department to grant Allen access to D.S.'s e-mail and voice mailbox accounts. Kelly stated that this was necessary in order to respond to customers that may have contacted D.S. and had not yet received a response.

**{¶ 7}** Kelly testified that a short time later, Allen reported that she had discovered an e-mail containing confidential client information that had been sent from D.S.'s Deep Green e-mail account to an outside e-mail address. Kelly

testified that upon reviewing the e-mail, she discovered that it had an attachment, which included information on Deep Green's customers that were in various stages of the loan application process. Kelly testified that she reported the discovery to Craig Rhodes, Deep Green's Human Resources Director.

**{¶ 8}** Kelly further testified that on August 11, 2005, she telephoned D.S. and asked her to come into the office to discuss a customer issue. Kelly testified that during the telephone conversation, D.S. was very combative and inquired if she was being fired. Finally, Kelly testified that D.S. promised to come into the office later that day to discuss the matter, but D.S. never did, and never reported to work thereafter.

**{¶ 9}** Randy Zuendel, Deep Green's former IT Security Manager, testified that on August 9, 2005, Deep Green's Human Resources Department asked him to investigate the e-mail that had been sent from D.S.'s Deep Green e-mail account to truloxs@hotmail.com. Zuendel testified that his investigation uncovered four separate e-mails sent from D.S.'s Deep Green e-mail account to outside e-mail addresses. Zuendel testified that one of the e-mails, sent March 9, 2005, had an attachment, which contained the names and account numbers of thousands of Deep Green's customers.

**{¶ 10}** Zuendel also testified an e-mail dated July 1, 2005, was sent to a second e-mail address, namely truloxs@yahoo.com. This e-mail was also sent to truloxs@hotmail.com. In addition, Zuendel testified the subject line of the e-

mail dated July 1, 2005, that was sent from D.S.'s Deep Green's e-mail account, was titled "note to myself." Further, this e-mail was written in the first person.

**{¶ 11}** Zuendel testified that the information contained in the e-mails sent from D.S.'s Deep Green e-mail account to the two outside e-mail addresses were proprietary in nature. Zuendel testified that if this proprietary information was disclosed to competitors or to other members of the public, it could significantly harm Deep Green's interests.

**{¶ 12}** Zuendel testified that pursuant to the Technology Security User's Guide, all electronic mail, including back-up copies, processed by Deep Green are considered the company's property. Zuendel testified that Deep Green's employees were also prohibited from uploading or downloading files from outside computers.

**{¶ 13}** Zuendel further testified that Deep Green's employees access their individual computers by utilizing a company-assigned user identification in conjunction with an employee-created password. Finally, Zuendel testified that the password to log onto the employee's computer is known only to that employee.

**{¶ 14}** At the close of the trial, the jury found D.S. not guilty of telephone communications fraud, but guilty of unauthorized use of computer and telecommunications property. On April 10, 2007, the trial court sentenced D.S. to one year of community control sanctions.

## Sufficiency of Evidence

**{¶ 15}** In the first assigned error, D.S. argues her convictions were not supported by sufficient evidence. We disagree.

**{¶ 16}** The sufficiency of the evidence standard of review is set forth in *State v. Bridgeman*:[1]

> Pursuant to Criminal Rule 29(A), a court shall not order an entry of judgment of acquittal if the evidence is such that reasonable minds can reach different conclusions as to whether each material element of a crime has been proved beyond a reasonable doubt.[2]

**{¶ 17}** *Bridgeman* must be interpreted in light of the sufficiency test outlined in *State v. Jenks*,[3] in which the Ohio Supreme Court held:

> An appellate court's function when reviewing the sufficiency of the evidence to support a criminal conviction is to examine the evidence submitted at trial to determine whether such evidence, if believed, would convince the average mind of the defendant's guilt beyond a reasonable doubt. The relevant inquiry is whether, after viewing the evidence in a light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime proven beyond a reasonable doubt. (*Jackson v. Virginia* (1979), 443 U.S. 307, 99 S.Ct. 2781, 61 L.Ed.2d 560, followed).

**{¶ 18}** In the instant case, the jury convicted D.S. for violating R.C. 2913.04, titled the "unauthorized use of property; computer, cable, or telecommunication property or service." R.C. 2913.04 provides in pertinent part as follows:

---

[1](1978), 55 Ohio St.2d 261, syllabus.

[2]See, also, *State v. Apanovitch* (1987), 33 Ohio St.3d 19, 23; *State v. Davis* (1988), 49 Ohio App.3d 109, 113.

[3](1991), 61 Ohio St.3d 259, paragraph two of the syllabus.

> (A) No person shall knowingly use or operate the property of another without the consent of the owner or person authorized to give consent.
>
> (B) No person, in any manner and by any means, including, but not limited to, computer hacking, shall knowingly gain access to, attempt to gain access to, or cause access to be gained to any computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service without the consent of, or beyond the scope of the express or implied consent of, the owner of the computer, computer system, computer network, cable service, cable system, telecommunications device, telecommunications service, or information service or other person authorized to give consent.
>
> * * *
>
> (D) The affirmative defenses contained in division (C) of section 2913.03 of the Revised Code are affirmative defenses to a charge under this section.

**{¶ 19}** The evidence adduced at trial established that D.S. knowingly utilized her access to Deep Green's computer system beyond the scope of the company's consent. The State presented testimony regarding four e-mails sent from D.S.'s Deep Green e-mail account to two unauthorized outside e-mail addresses. Three of the e-mails had attachments, and all the e-mails contained proprietary information. The subject line of one e-mail was titled "note to myself" and was written in the first person, clearly suggesting that the outside e-mail address belonged to D.S. D.S.'s transmittal of proprietary information from her Deep Green computer to the two unauthorized, outside e-mail addresses violated company's policy.

**{¶ 20}** In addition, the State presented testimony establishing that only D.S. could have transmitted the emails at issue. The record reveals that Deep Green's employees have an assigned user identification unique to them. The employee has to create a password, which is used in conjunction with their assigned user identification, to access their individual computer. Thus, only the employee can legitimately access their assigned computers.

**{¶ 21}** Further, our review of the Technology Security User's Guide reveals that employees are encouraged to change their passwords every forty-five days to provide a stronger measure of security. Finally, Zuendel, the IT Security Manager, testified that all e-mails received and sent to and from Deep Green are stored on the main exchange server.

**{¶ 22}** Zuendel testified as in pertinent part as follows about password security features and capabilities:

> Q. And who has access to these passwords?
>
> A. The account password were — that person is the only person who has access to that account.
>
> Q. So, if you personally wanted to access another employee's account, could you?
>
> A. I could access it using an administrative account, and I can take and copy records from that exchange server and I can copy them to another exchange box for review.
>
> Q. And by using an administrative account, what are you able to do with somebody else's file?
>
> A. From one inbox to another.

Q. Are you able to read another person's e-mail?

A. Yes.

Q. Are you able to send another person's e-mail?

A. You can send e-mail, you can reply to an e-mail that is contained in your inbox; however, it's going to use your log on. If I am logged in as an administrator account to copy that e-mail over and I reply to it, then it is going to have the administrator as the person sending the e-mail, not the originator of that e-mail.

Q. Okay. So, to be clear, if you are logging in as administrator and you want to reply to John Smith's e-mail that he received, will John Smith's name come up when you reply?

A. No. Administrator will come up, not John Smith.

Q. And it will say administrator?

A. Yes.

Q. And is there any way to send an e-mail as somebody else using the e-mail system at Deep Green?

A. They would need to have the user ID and password of that person.[4]

**{¶ 23}** Our review of the foregoing excerpt, and the evidence as a whole, viewed in a light most favorable to the State, indicates that there was sufficient evidence for the jury to determine the essential elements of the offense charged were proven beyond a reasonable doubt. Accordingly, we overrule the first assigned error.

[4]Tr. at 261-262.

## Manifest Weight of Evidence

**{¶ 24}** In the second assigned error, D.S. argues her conviction is against the manifest weight of the evidence. We disagree.

**{¶ 25}** In *State v. Wilson*,[5] the Ohio Supreme Court recently addressed the standard of review for a criminal manifest weight challenge, as follows:

> The criminal manifest-weight-of-the-evidence standard was explained in *State v. Thompkins* (1997), 78 Ohio St.3d 380, 1997 Ohio 52, 678 N.E.2d 541. In *Thompkins*, the court distinguished between sufficiency of the evidence and manifest weight of the evidence, finding that these concepts differ both qualitatively and quantitatively. *Id.* at 386, 678 N.E.2d 541. The court held that sufficiency of the evidence is a test of adequacy as to whether the evidence is legally sufficient to support a verdict as a matter of law, but weight of the evidence addresses the evidence's effect of inducing belief. *Id.* at 386-387, 678 N.E.2d 541. In other words, a reviewing court asks whose evidence is more persuasive -- the state's or the defendant's? We went on to hold that although there may be sufficient evidence to support a judgment, it could nevertheless be against the manifest weight of the evidence. *Id.* at 387, 678 N.E.2d 541. 'When a court of appeals reverses a judgment of a trial court on the basis that the verdict is against the weight of the evidence, the appellate court sits as a 'thirteenth juror' and disagrees with the factfinder's resolution of the conflicting testimony.' *Id.* at 387, 678 N.E.2d 541, citing *Tibbs v. Florida* (1982), 457 U.S. 31, 42, 102 S.Ct. 2211, 72 L.Ed.2d 652.

**{¶ 26}** As discussed in our resolution of the first assigned error, D.S.'s convictions were based on substantial and sufficient evidence. The testimony of Zuendel, Deep Green's IT Security Manager, established that D.S. was responsible for transmitting the e-mails, containing proprietary information, to

---

[5]113 Ohio St.3d 382, 2007-Ohio-2202.

the two unauthorized, outside e-mail addresses. D.S.'s actions were outside the scope of the access granted, and clearly violated Deep Green's policy. Therefore, D.S.'s convictions are not against the manifest weight of the evidence. Accordingly, we overrule the second assigned error.

**Admission of Evidence**

**{¶ 27}** D.S.'s remaining assigned errors encompass similar propositions of law regarding the admissibility of evidence; therefore, they will be addressed together.

**{¶ 28}** It is well-settled that the trial court has broad discretion in determining the admissibility of evidence.[6] Therefore, the trial court's ruling will not be disturbed absent an abuse of discretion. "The term 'abuse of discretion' connotes more than error of law or judgment; it implies that the trial court's attitude is unreasonable, arbitrary, or unconscionable."[7] When applying this standard of review, an appellate court must not substitute its judgment for that of the trial court.[8] Rather, reversal on appeal is warranted only when the trial court has exercised its discretion unreasonably, arbitrarily, or unconscionably.

---

[6]*State v. Delgado*, Cuyahoga App. No. 84152, 2004-Ohio-5865, citing *State v. Sage* (1987), 31 Ohio St.3d 173, paragraph two of the syllabus.

[7]*State v. Shepard*, Cuyahoga App. No. 81926, 2003-Ohio-3356, quoting *Blakemore v. Blakemore* (1983), 5 Ohio St.3d 217, 219.

[8]*State v. Reiner*, 93 Ohio St.3d 601, 2001-Ohio-1800, citing *Berk v. Matthews* (1990), 53 Ohio St.3d 161.

On review, this court considers whether the trial court abused its discretion and whether the complaining party has suffered material prejudice as a result.[9]

**Business Records Exception**

**{¶ 29}** First, D.S. argues that the trial court erred in admitting state's exhibits 1 through 4, the e-mails at issue, into evidence, under the business records exception to the hearsay rules. We disagree.

**{¶ 30}** Evid.R. 803(6), applicable herein, sets forth the "business records" exception to the hearsay rule and provides in pertinent part as follows:

> The following are not excluded by the hearsay rule, even though the declarant is available as a witness:
>
> * * *
>
> (6) Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of acts, events, or conditions, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness or as provided by Rule 901(B)(10), unless the source of information or the method or circumstances of preparation indicate lack of trustworthiness. * * *

**{¶ 31}** The Evidence Rules allow business records to be admitted into evidence if it can be shown by the testimony of either the custodian or some other qualified person that the record meets the specific safeguards of reliability identified in Evid.R. 803(6).[10] In addition, the phrase "other qualified witness"

---

[9]*State v. Long* (1978), 53 Ohio St.2d 91, 98.

[10]*State v. Patton* (Mar. 5, 1992), 3rdDist. No. 1-91-12.

should be broadly interpreted.[11] It is not necessary that the witness have firsthand knowledge of the transaction giving rise to the record.[12] Rather, it must be demonstrated that the witness is sufficiently familiar with the operation of the business and with the circumstances of the record's preparation, maintenance, and retrieval, that he can reasonably testify on the basis of this knowledge that the record is what it purports to be, and that it was made in the ordinary course of business consistent with the elements of Rule 803(6).[13]

**{¶ 32}** In his capacity as the IT Security Manager, Zuendel testified that all e-mails received or sent, including attached documents, are stored on Deep Green's exchange server in the normal and ordinary course of business. At trial, Zuendel testified in detail about the interface of the exchange server and an employee's workstation. Zuendel testified that all e-mails received or sent, first go through Deep Green's exchange server. The person receiving or sending an e-mail has to connect to the exchange server from their workstation through Microsoft Outlook in order to read or compose an e-mail.

**{¶ 33}** Zuendel testified that Deep Green conducts its business primarily through the internet and corresponds with their clients largely through e-mails. Thus, the record of all e-mail received or sent, including attached documents, are

---

[11]*Id.*

[12]*State v. Vrona* (1988), 47 Ohio App.3d 145.

[13]*State v. Shaheen* (July 29, 1997), 3rdDist. No. 5-97-03, citing *Patton, supra*.

kept in the normal course of business. Zuendel explained that once the e-mails were discovered, he was able to copy them from where they were stored on Deep Green's exchange server to a folder located on his computer. Zuendel testified that once the e-mails and attachments were copied to his computer, he printed the e-mails.

**{¶ 34}** We conclude that Zuendel's testimony demonstrated that he was familiar with the records of e-mails Deep Green kept in the ordinary course of business and the procedure to retrieve, transmit, and store the e-mails. Zuendel also had personal knowledge as to the retrieval of the e-mails after the discovery. Based on the foundation as established by Zuendel, the e-mails were admissible under the business records exception to the hearsay rule.

**Best Evidence Rule**

**{¶ 35}** Second, D.S. argues that a printout of the e-mails were not originals. We disagree.

**{¶ 36}** Pursuant to Evid.R. 1001(3), if data is stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original.[14]

**{¶ 37}** In the instant case, Zuendel testified that exhibits 1 through 4, the printed version of the e-mails, at issue, were stored on Deep Green's exchange server. Zuendel testified that the e-mails, including attachments, were retrieved

[14] *State v. Taylor*, 2nd Dist. No. 2005 CA 44, 2006-Ohio-6813.

from Deep Green's exchange server. Thus, the printout of the e-mails accurately reflects the data stored. Consequently, the trial court properly admitted exhibits 1 through 4 as originals.

**Exchange Server**

**{¶ 38}** Third, D.S. argues the trial court erred in admitting exhibits 1 through 4 without the State producing Deep Green's exchange server. We disagree.

**{¶ 39}** We have previously concluded that the printout of the four e-mails, at issue, are originals. Zuendel testified from personal knowledge that the e-mails were stored on the company's exchange server, and he produced the printed version of the e-mails from the exchange server. Consequently, the trial court properly admitted exhibits 1 through 4 into evidence. Accordingly, we overrule assigned errors three, four, and five.

Judgment affirmed.

It is ordered that appellee recover of appellant its costs herein taxed.

The court finds there were reasonable grounds for this appeal.

It is ordered that a special mandate be sent to said court to carry this judgment into execution. The defendant's conviction having been affirmed, any bail pending appeal is terminated. Case remanded to the trial court for execution of sentence.

A certified copy of this entry shall constitute the mandate pursuant to Rule 27 of the Rules of Appellate Procedure.

_____
PATRICIA ANN BLACKMON, JUDGE

JAMES J. SWEENEY, A.J., and
FRANK D. CELEBREZZE, JR., J., CONCUR