

IN THE SUPREME COURT OF OHIO

NATIONAL INTERSTATE	)	Supreme Court Case No. 2008-0757
CORPORATION, et al.,	)	
	)	On Appeal from the Summit County
Appellees,	)	Court of Appeals, Ninth Appellate
	)	District
vs.	)	
	)	Court of Appeals Case No. 07-CA-
ANDREW WEST, et al.,	)	23877
	)	
Appellants.	)	

---

MEMORANDUM IN SUPPORT OF JURISDICTION

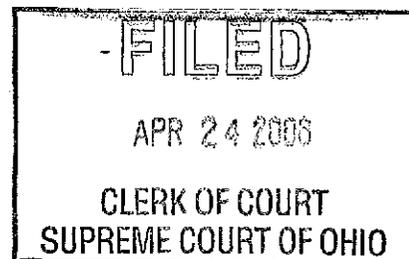
---

John H. Schaeffer (S.Ct. #0041874) (COUNSEL OF RECORD)  
Susan E. Baker (S.Ct. #0059569)  
Critchfield, Critchfield & Johnston, Ltd.  
225 North Market Street, P.O. Box 599  
Wooster, OH 44691  
Phone: (330) 264-4444; Fax: (330) 263-9278  
Email: [schaeffer@ccj.com](mailto:schaeffer@ccj.com); [baker@ccj.com](mailto:baker@ccj.com)

Timothy Whitford (S.Ct. #0059954)  
Ritzler, Coughlin & Swansinger, Ltd.  
1360 East Ninth Street, 1000 IMG Center  
Cleveland, OH 44114  
Phone: (216) 241-8333; Fax: (216) 241-5890  
Email: [twhitford@rcs-law.com](mailto:twhitford@rcs-law.com)

COUNSEL FOR APPELLANTS

Christopher R. Johnson (S.Ct. #0072995) (COUNSEL OF RECORD)  
Timothy H. Linville (S.Ct. #0076819)  
Thompson Hine, LLP  
3900 Key Center, 127 Public Square  
Cleveland, OH 44114  
Phone: (216) 566-5500; Fax: (216) 566-5800  
Email: [chris.johnson@thompsonhine.com](mailto:chris.johnson@thompsonhine.com); [tim.linville@thompsonhine.com](mailto:tim.linville@thompsonhine.com)



## TABLE OF CONTENTS

	<u>Page</u>
EXPLANATION OF WHY THIS IS A CASE OF PUBLIC OR GREAT GENERAL INTEREST AND INVOLVES A SUBSTANTIAL CONSTITUTIONAL QUESTION .....	1
STATEMENT OF THE CASE AND FACTS .....	4
ARGUMENT IN SUPPORT OF PROPOSITIONS OF LAW .....	8
<u>Proposition of Law No. 1:</u> A decision by a trial court to require one party to produce its computers and other electronic devices to a business rival for forensic examination is a final appealable order .....	8
<u>Proposition of Law No. 2:</u> Cloning, or forensic examination, of another party's computers and personal technology devices should be ordered as a last resort, and only after the requesting party has made a threshold showing that (a) they have evidence that the information desired is on the other party's computers, and (b) that the requesting party has exhausted less intrusive means of discovering the information sought.....	13
CONCLUSION .....	14
PROOF OF SERVICE .....	15
APPENDIX	<u>Appx. Page</u>
Opinion of the Summit County Court of Appeals (March 12, 2008) .....	1
Protective Order Governing Imaging, Inspection of Computers and Electronic Devices, Protection of Confidential and Privileged Information and Preservation of Privilege in the Event of Inadvertent Production of Privileged Material (Summit County, August 27, 2007).....	12
Order Regarding Protection of Confidential Information (Summit County, August 27, 2007).....	20

EXPLANATION OF WHY THIS CASE IS A CASE OF  
PUBLIC OR GREAT GENERAL INTEREST AND  
INVOLVES A SUBSTANTIAL CONSTITUTIONAL QUESTION

This case presents a critical issue for the future of electronic discovery in Ohio. The main issue is when is it permissible to allow one company to perform a forensic examination on the computers and other electronic devices of a business rival and potential competitor. The sub-issue is whether an order from a trial court requiring the rival to submit to the cloning and forensic examination is a final appealable order under R.C. § 2505.02(B)(4).

In this case, the Ninth District Court of Appeals ignored the action of the forensic examination itself, and instead focused on the documents that would eventually be produced in hard copy form following the forensic examination. Deciding that the trial court has not been presented with the opportunity to determine whether any particular documents to be produced following the examination constitute trade secrets, the Court of Appeals held that the order of the trial court was not a final appealable order because it neither determined the action with respect to the provisional remedy nor prevented judgment in the action in favor of the appealing party with respect to the provisional remedy.

The decision of the Court of Appeals threatens all small businesses and individuals in Ohio as the cost to clone computers can run in the tens of thousands of dollars. Most small businesses and individuals cannot afford to meet the cost of the discovery. Unfortunately, the Ninth District's decision states that there is no right to appeal until these great expenses are first incurred. Many small businesses may simply cease to exist once a suit of this nature is filed by their rivals, and individuals may have to declare bankruptcy simply to defend themselves if sued by a former employer.

The decision from the Ninth District Court of Appeals further threatens all businesses, large

and small, wishing to protect their computer systems and other electronic devices from invasion and inspection by a rival company. By focusing solely on the hard copy version of the documents which may be produced at the end of the examination, the Court of Appeals missed the devastating impact to a young, start-up company of having an adversary gain access to the business and its computer system. The Court of Appeals ignored the damage the forensic examination could cause to the new company's computers. The Court of Appeals failed to identify the reality that the adversary would gain access to the new company's confidential, proprietary and trade secret information, prior to the trial court having an opportunity to rule upon whether the adversary is entitled to view the hard copy form of the documents. Finally, the Court of Appeals failed to seize the opportunity to set forth a standard of proof that trade secret plaintiffs must meet prior to being granted the authority to scan and duplicate a business rival's computers.

With electronic discovery becoming more prevalent, including the recent revision of the Ohio Rules of Civil Procedure to address electronic discovery, this Court is now presented with an opportunity to remedy the failures of the Court of Appeals and set forth a standard that will provide a framework for future cases involving a business wishing to clone the computers and other electronic devices of another. As it currently stands from the extremely low threshold required by the trial court, as well as the Court of Appeals' failure to address the real issue, future cases will most certainly arise. Although this case occurred under the current, and soon to be former, Ohio Rules of Civil Procedure, the issues involved in this case are applicable and relevant to the cases this Court will see in the future under the new rules. Thus, this case can serve as a guide to all litigants in Ohio as to what is permissible, and what thresholds must be met when the issues of cloning business computers and personal devices are raised.

Rather than seizing the opportunity to address these issues and concerns, the Court of

Appeals was limited in its vision and focused only on the narrow issue of the production of the hard copy versions of any documents contained on the computer. That view of electronic discovery is anachronistic and myopic. It is the access to the computers and other electronic devices that is relevant because that data can be viewed and printed by the party doing the scanning without any production of documents by the other company. In doing so, the adversary company would gain access to confidential, proprietary and trade secret information and the damage would be done. If the trial court then later ruled that the information should not be disclosed in hard copy form, it would be too late to undo the harm. The company being examined would have no judicial redress for the injury, and its Due Process rights would be violated.

Ohio law encourages competition. This case, as it currently stands, would have a chilling effect on competition. If an individual left one company and went to another in the same or similar industry, the former company could conduct a forensic examination of the new company's computer systems to search for allegedly misappropriated "trade secrets." It is the examination itself, the cloning of the computers, that is the key, and not necessarily the hard copy version of the documents contained on the system. That alone should scare any business in Ohio. Moreover, such a threat would deter individuals from exhibiting the initiative of leaving their current employment to start their own businesses. Therefore, a majority of Ohioans are affected by the issues in this case and it should easily meet the threshold requirement of public or great interest.

This case involves a substantial constitutional question in that the failure of the Court of Appeals to address the issue denies the Appellants their due process rights under Article I, Section 16 of the Ohio Constitution. Injury will occur to the Appellants and they will be without remedy by due course of law, and will be denied justice.

In sum, this case puts in issue what protections are afforded to a business' computer system

and other electronic devices, thereby affecting every business in Ohio. As personal computers and electronic devices are also requested, virtually every person in Ohio is affected. To promote and preserve the integrity of proprietary, confidential and trade secret information, to set forth a standard or threshold a trade secret plaintiff must meet prior to being permitted to have access to and clone a rival's computers, and to set forth a guide for all future electronic discovery cases to follow, this Court must grant jurisdiction to hear this case and review the erroneous and dangerous decision of the Court of Appeals.

### **STATEMENT OF THE CASE AND FACTS**

The case arises from the attempts of Appellees National Interstate Corporation ("NIC") and its subsidiary, National Interstate Insurance Company ("NIIC") to stop individual Appellants Andrew West, Eric J. Raudins, William Hobbs, and Scott Gurley, as well as corporate Appellants RIS Holdings, LLC, Recreation Insurance Specialists, LLC, RIS Risk Management Services, LLC, and RIS Holdings Corporation (hereinafter the "RIS entities"), from doing business which would compete in the same market as NIIC.

NIIC is an insurance company, which insures recreational vehicles ("RV") and other personal lines products. Raudins was a Vice-President overseeing those products and Hobbs was the Product Manager of the RV product. Raudins and Hobbs left NIIC in early 2006. Hobbs subsequently formed the RIS entities while Raudins worked on his own side-company, Corvette Chrome, LLC. While both Raudins and Hobbs had Non-Compete and Confidentiality agreements with NIIC, it is without argument that neither Hobbs' formation of the RIS entities nor Raudins' work at Corvette Chrome violated those agreements. In February 2007, when his non-compete agreement expired, Raudins invested in the RIS entities and later became the Chief Operating Officer. One of the RIS entities hired West to serve as an information technology ("IT") analyst. Based upon his prior IT

experience, such a position would not violate the non-competition agreement West had with NIIC, which prohibited him from working for an “insurer” in a role that was similar to his position at NIIC as Product Manager of the RV product. The RIS entities are not “insurers” and West’s IT role was not a managerial position over RV insurance. Thus, the Appellants felt that the hire did not violate the terms of West’s agreement with NIIC.

NIC filed its Complaint on March 1, 2007 against West, Raudins, Hobbs and the RIS entities alleging misappropriation of trade secrets and violation of their non-compete agreements. Simultaneously, NIC moved for a temporary restraining order (“TRO”) and preliminary injunction against West to prohibit him from ever working for the RIS entities. The trial court granted NIC’s TRO on March 7, 2007 and scheduled a hearing before Magistrate Shoemaker on the motion for preliminary injunction for March 16, 2007. The trial court also granted a motion for expedited discovery requiring Appellants to respond to interrogatories and requests for production of documents by March 12, and for depositions to occur on March 13. NIC served its requests for production of documents upon Appellants on March 5, 2007. Those requests sought, among other things, production of electronic documents and communications as well as production of Appellants’ corporate and personal computers for examination.

- Appellants filed a Motion for Protective Order and Motion to Quash on March 12, 2007 seeking an exemption from the obligation to provide certain documents and communications relating to business plans, subscription agreements and operating agreements, as well as the production of the computers and electronic devices. After NIC responded, the trial court ordered that e-mail communications had to be turned over, but held all other requests in abeyance because they were “overly broad, overly burdensome, and may contain trade secrets and/or other confidential information.” (March 14, 2007 Order). The trial court stated that NIC could renew its request after

the parties discussed a stipulated protective order.

The preliminary injunction hearing occurred on March 21 and 22, and on April 4, 2007, Magistrate Shoemaker issued an Order recommending that the trial court grant the preliminary injunction prohibiting West from working with the RIS entities for one year. Importantly, although there was evidence that West had sent some e-mails to Hobbs after Hobbs left NIIC, Magistrate Shoemaker issued his recommendation despite finding that “there is no evidence that Mr. West has passed on to Defendant RIS any proprietary information or trade secrets of Plaintiff.” (Magistrate’s Decision at Findings of Fact ¶ 12). On August 10, 2007, the trial court finally adopted the Magistrate’s Order over the written objections of the Appellants.

In the meantime, NIC amended its complaint to add NIIC as a party-plaintiff, and added Gurley, who had at one time been a NIIC employee, as an individual defendant. Appellees requested a preliminary injunction prohibiting Gurley from working for the RIS entities, but have never pursued the matter further. Gurley provided documents to Appellees, and the agency that Gurley worked for after leaving NIIC also provided documents, but Gurley has not been deposed.

In June, three months after the initial protective order, the parties began discussions on a stipulated protective order. The parties agreed to all the proposed language with the exception that Appellants would not agree to produce their business plans, subscription agreements or operating agreements. There was no language in the proposed stipulated protective order regarding the cloning or forensic examination of computers, nor was such a matter ever discussed between the parties. A conference call to resolve the dispute about the business plan and other agreements in the proposed protective order occurred with the trial court on June 29, 2007. The discussion involved the types of documents that Appellants did not want to produce, and Appellees’ counsel’s assurances that only counsel would see them. At one point, the trial court judge stated that while Appellees’ counsel’s

promises as to confidentiality were commendable, practically speaking, Appellants' confidential documents would eventually be seen by others. Nevertheless, the trial court ordered the simultaneously filing of briefs on the issue.

Appellants' brief noted that the written discovery of Appellees included requests for trade secrets, as well as confidential and proprietary information that if disclosed, would seriously injure Appellants. Furthermore, Appellants reiterated their point that Appellees' allegedly misappropriated confidential information was publicly available, did not constitute "trade secrets," and Appellants could not have misappropriated the information as a matter of law.

In their brief, Appellees ambushed Appellants with the proposal to do a comprehensive cloning of the RIS entities' corporate computers and the personal computers and electronic devices of the individual Appellants, a subject not discussed in the June 29 conference. Appellees further requested a protective order requiring such a submission. Without noting the completely different styles of the briefs, or holding any further oral argument, the trial court adopted Appellees' proposed order on August 10, 2007, and that order was finalized on August 27, 2007. The Order provided that once the cloning was done, Appellants' counsel had only ten (10) days to review and redact any matters deemed to be protected by the attorney-client privilege, work product doctrine, and all other private, privileged, proprietary and confidential matters. At the conclusion of ten days, all matters not yet reviewed would be required to be turned over to Appellees, whether or not the material is privileged, confidential, etc. The Order further required that Appellees have unfettered access to all corporate and personal computers and electronic devices, and that Appellants are not permitted to be present unless they pay Appellees' expert's exorbitant fees. Appellants have no say in any search terms, the preservation of the cloned machines, or the destruction or return of confidential and privileged information.

Appellants appealed the trial court's granting of the Appellees' protective order, and the order permitting the Appellees the ability to clone and forensically examine Appellants' computers. After the filing of the Notice of Appeal, Appellees filed a Motion to Preserve Electronic Data and Motion for a Temporary Restraining Order and Preliminary Injunction seeking to restrain Appellants from using any of their computers or electronic devices during the appeal. Those motions were denied.

The Court of Appeals, after briefing and argument, issued an opinion stating that the appeal was not based upon a final appealable order.

### **ARGUMENT IN SUPPORT OF PROPOSITION OF LAW**

**Proposition of Law No. 1: A decision by a trial court to require one party to produce its computers and other electronic devices to a business rival for forensic examination is a final appealable order.**

Oddly enough, it is a Ninth District opinion that summarizes final appealable orders as they pertain to discovery matters. In *Gibson-Myers & Associates, Inc. v. Pearce*, Summit Co. Case No. C.A. No. 19358, October 27, 1999, 1999 Ohio App. LEXIS 5010, the court noted that "as a general rule, orders regarding discovery are interlocutory and not immediately appealable." *Id.* at \* 3 (citation omitted). Nevertheless, the court realized that changes in the Ohio Revised Code had created several exceptions.

Those changes can be found in R.C. § 2505.02, which defines "final orders." Specifically, section (B) states, in pertinent part:

An order is a final order that may be reviewed, affirmed, modified, or reversed, with or without retrial, when it is one of the following:

\* \* \*

(4) An order that grants or denies a provisional remedy and to which both the following apply:

(a) The order in effect determines the action with respect to the provisional remedy and prevents a judgment in the action in favor of the appealing party with respect to the provisional remedy.

(b) The appealing party would not be afforded a meaningful or effective remedy by an appeal following final judgment as to all proceedings, issues, claims, and parties in the action.

A “provisional remedy” is defined as “a proceeding ancillary to an action, including, but not limited to, a proceeding for a preliminary injunction, attachment, discovery of privileged matter, or suppression of evidence.” R.C. 2505.02(A)(3). Prior to this change, a discovery order was a final appealable order only if the potential damage from the order was incapable of later correction. *Doe v. Univ. of Cincinnati* (1988), 42 Ohio App. 3d 227, 538 N.E.2d 419. Now, under the revised language, an order for the production of privileged information is a provisional remedy under R.C. 2502.02. *Whitt v. ERB Lumber* (2004), 156 Ohio App. 3d, 518, 806 N.E.2d 1034, 2004 Ohio 1302.

The *Gibson-Myers* opinion also discussed trade secrets at some length. The Ninth District stated that “it is axiomatic that documents containing privileged information or those constituting trade secrets are exempt from disclosure.” *Gibson-Myers, supra*, at \*6 (citations omitted). “Just as the phrase “provisional remedy” encompasses the discovery of privileged material, it should also be read to include the discovery of confidential information, i.e. trade secrets.” *Id.* The Ninth District realized the importance of protecting trade secrets as it went on to state:

On its face, R.C. 2505.02(A)(3) is flexible and able to address situations where a party has a protectable interest at stake and yet has no meaningful ability to appeal the decision which discloses that interest to others. If a trial court orders the discovery of trade secrets and such are disclosed, the party resisting discovery will have no adequate remedy on appeal. The proverbial bell cannot be unrung and an appeal after final judgment on the merits will not rectify the damage. In a competitive commercial market where customers are a business’ most valuable asset and technology changes daily, disclosure of a trade secret will surely cause irreparable harm.” *Id.* at \* 6-7.

This situation, in which a trial court denies a protective order and allows access to privileged documents, is recognized by other districts as one involving a final appealable order. *See Sirca v. Medina County Dept. of Human Services* (Medina Co. 2001), 145 Ohio App. 3d 182, 762 N.E.2d 407 (trial court's denial of motion for protective order as to medical record and testimony of treating mental health professionals was final appealable order); *Armstrong v. Marusic*, Lake App. No. 2001-L-232, 2004 Ohio 2594 (court's order allowing plaintiff to inspect information containing defendant's trade secrets was final appealable order because once information was disclosed defendant would not have an effective remedy); *Schottenstein, Zox & Dunn v. McKibben*, Franklin App. No. 01AP-1384, 2002 Ohio 5075 (court's order allowing discovery of attorney's client file was final appealable order because no meaningful review possible once information is disclosed). As these courts and others have noted, once privileged or confidential information is disclosed, the party resisting discovery has no adequate remedy on appeal. *See also Williams v. Nationwide Mutual Ins. Co.*, Meigs App. Case No. 05CA15, 2005 Ohio 6798.

Thus, while the Ninth District understood the history of the issue involved in this case, it failed to adapt its thinking to keep up with the ever-changing technology, as well as the inventiveness of the Appellees' attorneys' requests. Here, Appellees have not only requested production of documents, but access to Appellants' corporate and personal computers and other electronic devices in order to examine them and clone them. One request involves the production of hard copy documents, many of which would contain trade secrets and other confidential information. The other involves gaining access and making a copy of data that has not yet been reduced to paper form.

The Ninth District may have been correct that until such time as the trial court rules on Appellees' request for the production of certain hard copy documents to which Appellants object, there may not be a final appealable order. But that position only focuses on half of the request, and

by extension, half the problem. By requesting and obtaining the opportunity to examine and clone Appellants' computers and other electronic devices, Appellees have essentially eliminated the need to ask for hard copy versions of the documents. In other words, the proverbial bell will be rung upon examination of the computers, not the production of the documents. Because the Ninth District did not grasp the relevance of the forensic examination, they erred in holding that they lacked jurisdiction to decide the appeal.

While the issues surrounding computer forensic experts and electronic discovery are relatively new due to advances in technology, the Southern District of Ohio has examined this issue in relation to the new Federal electronic discovery rules in *Scotts Company LLC v. Liberty Mutual Insurance Company* (June 12, 2007), S.D. Ohio Case No. 2:06-CV-899, 2007 U.S. Dist. LEXIS 43005. In *Scotts*, the court addressed the issue in the form of a Motion to Compel and request for a protective order that is substantially similar to the protective order issued in the instant matter. The plaintiff in *Scotts* sought to compel electronic discovery conducted by a computer forensic company, in which the company would make a forensic clone of the defendant's computer systems and conduct a search of the clone using various search terms. In *Scotts*, much like this matter, the plaintiff offered to enter into a protective order permitting the defendant to have 10 days to review any materials pulled in the electronic search to determine whether or not the documents were subject to privilege.

The *Scotts* Court found that without a qualified reason, even under the new Federal electronic discovery rules, "a plaintiff is no more entitled to access to defendant's electronic information storage systems than to defendant's warehouses storing paper documentation." *Scotts* at \* 5. The Court explained that the process is designed to be extrajudicial and relies upon the responding party to produce the requested information. The court, quoting *Deipenhorst v. City of Battle Creek*, Case

No. 1:05-cv-734, 2006 U.S. Dist. LEXIS 48551, \*10-11 (W.D. Mich. June 30, 2006) cautioned:

In the absence of a strong showing that the responding party has somehow defaulted in this obligation, the court should not resort to extreme, expensive, or extraordinary means to guarantee compliance. Imaging of computer hard drives is an expensive process, and adds to the burden of litigation for both parties, as an examination of a hard drive by an expert automatically triggers the retention of an expert by the responding party for the same purpose. Furthermore, as noted above, imaging a hard drive results in the production of massive amounts of irrelevant, and perhaps privileged, information.

*Scotts* at \* 5. The *Diepenhorst* court was “loathe to sanction intrusive examination of an opponent’s computer...on the mere suspicion that the opponent may be withholding discoverable information” because such suspicions and conduct are possible in every case yet courts do not allow the plaintiff to intrude onto a defendant’s premises to go through paper files to verify all discovery was turned over and therefore they should not be permitted to do so with the electronic files. *Id.*

The Southern District of Ohio further examined how other various Federal courts in the United States handled similar requests for electronic discovery. Many courts, who have examined electronic discovery issues regarding imaging of an opponent’s computer, do not grant a routine right to access such electronic files without evidence that the opposing party is withholding information. The Court noted that the Federal rules merely provide for a party to search its own information and provide relevant data but does not give the requesting party the right to conduct its own search.

One such case was *Bethea v. Comcast*, 218 F.R.D. 328 (D.C. Dist. 2003), which involved a claim of employment discrimination. The employee sought to inspect the employer’s computer systems and programs the employee believed that there should be numerous documents relating to a massive reorganization that had not been turned over during discovery. The employer denied that these documents existed and claimed to have already produced all relevant data in paper format. The court found that the employee failed to show that the employer had destroyed or unlawfully withheld

any documents and therefore the imaging of the computer was unwarranted.

A similar threshold showing needs to be in place in Ohio. Having someone dismantle your computer to copy the hard drive is not without risk. One does not need to be a computer expert to know that anytime one tampers with such a device, a problem may result. This is especially true if the hard drive is to be delivered to an off-site location as the mere jiggling, rattling or accidental dropping of it could result in a complete data loss. Once the scanning is completed, Appellees' agents will be in possession of Appellants' most confidential, proprietary and essential business data, as well as massive amount of irrelevant information, including personal data, to which Appellees have no right to discovery under the Civil Rules. Thus, the act of cloning is a final appealable order and this Court should accept jurisdiction of this matter.

**Proposition of Law No. 2: Cloning, or forensic examination, of another party's computers and personal technology devices should be ordered as a last resort, and only after the requesting party has made a threshold showing that they have evidence that (a) the information desired is on the other party's computers, and that (b) the requesting party has exhausted less intrusive means of discovering the information sought.**

While the focus of Appellants' appeal is the Ninth District's decision that the trial court's order was not a final appealable order, the issues involving the finality of the order for the cloning of the computers are intertwined with the issue of fundamental fairness. The trial court's orders sanction the equivalent of permitting a party opponent to wholesale warehouse access to all of the business information of a rival without a preliminary showing of relevance, need or good cause. Further, the alleged "safeguards" are illusory. Appellants believe that this case is of public and great general interest, and if jurisdiction is accepted, both sides will undoubtedly argue both issues. For

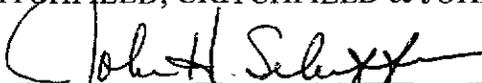
that reason, Appellants incorporate by reference arguments made in Proposition of Law No. 1 relating to the standards or thresholds for permitting cloning of computers as if fully rewritten herein, and request that the Court consider this issue as well.

### CONCLUSION

In this case, Appellees can neither state what "trade secret(s)" were allegedly misappropriated, nor can they establish that any non-privileged or non-confidential information requested in discovery was not provided to them. Thus, the Appellees' discovery requests for the electronic records of the RIS entities and the individual Appellants, which seeks the trade secrets of the RIS entities, are nothing more than an impermissible fishing expedition conducted by one business against another in an effort to squash any potential competition. In other words, Appellees' request to access the Appellants' computers and personal electronic devices is a predatory discovery tactic designed to drive a rival out of business. Once the cloning occurs and the data is no longer in the sole possession of the Appellants, there will be no remedy or relief that any court could provide to the Appellants from the eventual and inevitable disclosure of that information. The proverbial bell will be rung once the cloning and forensic examination is performed. This is the key point which the Ninth District overlooked and failed to consider. This Honorable Court has the opportunity to address the issue of computer cloning and forensic examination and set forth a guideline for all future cases that will be applying the new e-discovery rules. For all of the above reasons, Appellants respectfully request that the Supreme Court accept jurisdiction of this matter.

Respectfully submitted,

CRITCHFIELD, CRITCHFIELD & JOHNSTON, LTD.

By: 

John H. Schaeffer (S.Ct. #0041874)

Susan E. Baker (S.Ct. #0059569)

Attorneys for Defendants

225 North Market Street, P.O. Box 599

Wooster, OH 44691

Phone: 330-264-4444; Fax: 330-263-9278

Email: [schaeffer@ccj.com](mailto:schaeffer@ccj.com); [baker@ccj.com](mailto:baker@ccj.com)

RITZLER, COUGHLIN & SWANSINGER, LTD.

By: /s/ Timothy Whitford (per e-mail consent)

Timothy Whitford (S.Ct. #0059954)

1360 East Ninth Street, 1000 IMG Center

Cleveland, OH 44114

Phone: (216) 241-8333; Fax: (216)241-5890

Email: [twhitford@rcs-law.com](mailto:twhitford@rcs-law.com)

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing Memorandum In Support of Jurisdiction was served by regular U. S. Mail this 23rd day of April, 2008 to:

Christopher R. Johnson, Esq.

Timothy Linville, Esq.

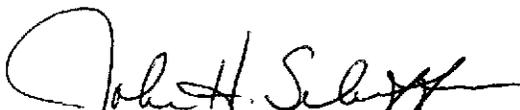
THOMPSON HINE, LLP

3900 Key Center

127 Public Square

Cleveland, OH 44114

*Attorneys for Appellees*

  
\_\_\_\_\_  
John H. Schaeffer  
Counsel for Appellants



## FACTS

{¶2} National Interstate Corporation is an insurance company that provides, among other things, specialized insurance policies for recreational vehicles. Mr. Hobbs, Mr. West, and Mr. Raudins are all former employees of NIC who had been employed subject to noncompetition agreements. Mr. Hobbs created the RIS entities, which later employed both Mr. West and Mr. Raudins. On March 1, 2007, National Interstate Corporation and National Interstate Insurance Company (collectively, "NIC") filed this action against RIS alleging claims of breach of contract and misappropriation of trade secrets. NIC also alleged claims of breach of a duty of loyalty against Mr. West and tortious interference with business relationships against the RIS entities, Mr. Raudins, and Mr. Hobbs. The crux of NIC's complaint is the allegation that the RIS entities, Mr. Hobbs, and Mr. Raudins used trade secrets of NIC to further their plan to form a competing business and used Mr. West - the last of the three to leave NIC's employ - to obtain trade secrets at NIC's expense.

{¶3} The trial court expedited discovery and, on March 5, 2007, NIC served discovery requests upon RIS. Of particular relevance to this appeal is NIC's request, propounded upon defendants West, Raudins, and Hobbs, for "all computer, cellular phone, personal data assistants and any other device or other device from which you are able to send emails, text messages or other electronic communications." NIC also requested documents related to West, Hobbs,

Raudins, and RIS's "business plans, operations and strategies." On March 12, 2007, RIS moved for a protective order, specifically objecting to NIC's Requests for Production of Documents by Mr. West, numbered one, four, five, eight, and nine; by the RIS entities, numbered five, six, and nine; and by Mr. Raudins and Mr. Hobbs, numbered one, four, five, and eight through ten. RIS objected to each of these requests on the basis that they requested the disclosure of trade secrets, and raised various objections based on overbreadth and relevancy of the information sought by NIC. In response to NIC's request to examine their devices capable of sending electronic communications, RIS objected:

"In response to this request, RIS maintained that "[i]f the Court were to enforce this request, Defendant[s] would basically have to request everything [they] have which is capable of storing electronic communications and allow Plaintiff to figure out what was relevant, privileged, or otherwise protected, all the while looking through everything which is not."

{¶4} NIC responded in opposition to the motion for protective order on March 14, 2007. In response to RIS's objection to the request for devices capable of sending electronic communications, NIC argued:

"Defendants, by asserting that 'not everything' on the requested devices is relevant, admit that the devices contain relevant information. Despite that fact, Defendants are entirely refusing to respond to this Request. In doing so, Defendants are flaunting their obligations under the Ohio Rules. Moreover, it is not for Defendants to pick and choose what information is relevant and what is not. \*\*\* [T]he existence of some irrelevant information does not mean that Defendants can make a blanket refusal to produce the requested information.

“It is anticipated that information that incriminates Defendants is contained on the devices requested, and the only way to get that information very likely is through a forensic examination of the devices. After all, it is likely that Defendants have deleted any communications or other information. Additionally, Plaintiffs have very good reason to believe that the individual Defendants \*\*\* used personal email accounts to communicate and transfer Plaintiff’s trade secret information. The personal email account information and evidence of those communications would necessarily be contained on the Defendant’s computers and personal communication devices.” (Emphasis added.)

NIC also stated that it would agree to a protective order that required the production of the requested items, but subject to RIS’s ability to designate certain information as “for attorney’s eyes only.”

{¶5} On July 5, 2007, the trial court ordered the parties to “simultaneously file their briefs on the issue of Defendants’ business plans, financial documents, operational agreements, and related matters by July 9, 2007.” It appears from the record that, prior to filing their briefs, the parties engaged in negotiations regarding an agreed protective order. The negotiations, however, broke down short of an agreement. The parties filed simultaneous briefs on that date related to the previously-filed motion for a protective order. The trial court did not conduct a hearing, nor did RIS provide any documents to the trial court for an in camera inspection. Instead, the responses related to NIC’s discovery requests in general and in their entirety, not to specific documents identified by either party. RIS argued that its trade secrets could only be protected by an order that blocked all of NIC’s discovery requests which covered trade secrets; NIC

maintained that RIS's trade secrets -- if any -- could be adequately protected by a protective order restricting access to documents designated in the course of production. NIC also reiterated its position that a forensic examination of RIS's computers was necessary to obtain the discovery documents and to protect them from destruction.<sup>1</sup>

{¶6} The trial court denied RIS's motion for a protective order prohibiting the discovery, but concluded that NIC's proposed protective order was appropriate under the circumstances. The trial court also found that a forensic examination of RIS's computers was warranted and ordered NIC to provide a protocol for the examination. On August 27, 2007, the trial court adopted NIC's proposed protective order and imaging protocol. RIS has appealed from those orders, asserting that they are within this Court's jurisdiction pursuant to R.C. 2505.02(B)(4).

JURISDICTION

{¶7} Section 3(B)(2), Article IV of the Ohio Constitution grants courts of appeals the jurisdiction "to review and affirm, modify, or reverse judgments or final orders[.]" R.C. 2505.02(B) includes within the scope of our jurisdiction

---

<sup>1</sup> RIS did not address the forensic examination of its computers in its supplemental brief, despite the fact that NIC raised the issue at least three months before in response to the motion for a protective order. On the facts of this case, this court makes no determination with respect to whether an order compelling a forensic computer analysis, standing alone, meets the requirements of R.C. 2505.02(B)(4).



certain interlocutory orders. Among these are orders that grant or deny a provisional remedy, or “a proceeding ancillary to an action, including, but not limited to, \*\*\* discovery of privileged matter[.]” R.C. 2505.02(A)(3). R.C. 2505.02 (B)(4) provides:

An order is a final order that may be reviewed, affirmed, modified, or reversed, with or without retrial, when it \*\*\* grants or denies a provisional remedy and to which both of the following apply:

- (a) The order in effect determines the action with respect to the provisional remedy and prevents a judgment in the action in favor of the appealing party with respect to the provisional remedy.
- (b) The appealing party would not be afforded a meaningful or effective remedy by an appeal following final judgment as to all proceedings, issues, claims, and parties in the action.

{¶8} A determination that an order relates to a provisional remedy, however, is only the first step in determining this court’s jurisdiction under R.C. 2505.02(B)(4). See *Sinnott v. Aqua-Chem, Inc.*, 116 Ohio St.3d 158, 2007-Ohio-5584, at ¶16; *State v. Muncie* (2001), 91 Ohio St.3d 440, 450. “R.C. 2505.02(B)(4) establishes a three-part test for determining whether an order is final and appealable. As an initial matter, the order must grant or deny a provisional remedy; if so, the order must also determine the action and prevent a judgment in favor of the appealing party regarding the provisional remedy, and the appealing party cannot have a meaningful or effective appellate remedy following final judgment. *Not all provisional remedy orders are necessarily appealable; the conditions of R.C. 2505.02(B)(4)(a) and (b) must be satisfied before the order can*

*be considered final and appealable.*" (Emphasis added.) *Sinnott*, at ¶16, citing *Muncie*, 91 Ohio St.3d at 446, 450. See, also, *Briggs v. Mt. Carmel Health Sys.*, 10th Dist. No. 07AP-251, 2007-Ohio-5558, at ¶12;

{¶9} This court has determined that an order which compels the discovery of trade secrets may be final and appealable as a provisional remedy. *Gibson-Myers & Assoc. v. Pearce* (Oct. 27, 1999), 9th Dist. No. 19358, at \*2. In that case, we concluded:

"On its face, R.C.2505.02(A)(3) is flexible and able to address situations where a party has a protectable interest at stake and yet has no meaningful ability to appeal the decision which discloses that interest to others. If a trial court orders the discovery of trade secrets and such are disclosed, the party resisting discovery will have no adequate remedy on appeal. The proverbial bell cannot be unrung and an appeal after final judgment on the merits will not rectify the damage. In a competitive commercial market where customers are a business' most valuable asset and technology changes daily, disclosure of a trade secret will surely cause irreparable harm." *Id.*

Other cases, however, illustrate the need for flexibility in application of R.C. 2505.02(A)(3) with respect to the facts of each case and the stage of discovery at which the parties find themselves. Along this spectrum lie orders which relate to the discovery of trade secrets – and, therefore, to a provisional remedy – but which do not meet the requirements of R.C. 2505.02(B)(4)(a) and (b) with respect to the discovery.

{¶10} In *Dispatch Printing Co. v. Recovery Ltd. Partnership*, 10th Dist. Nos. 05AP-640, 05AP-691, 05AP-731, 2006-Ohio-1347, the Tenth District Court of Appeals considered an order that granted a motion to compel, denied a motion

for a protective order, and allowed discovery with respect to trade secrets. In that case, however, “the trial court envisioned more than just completely unrestricted discovery. \*\*\* In effect, the trial court did not simply order the production of proprietary or trade-secret information, but, rather, it ordered that discovery should continue with safeguards in place in order to address the concerns regarding proprietary information or trade secrets[.]” *Id.* at ¶12. The court held that the trial court’s order related to regulation of discovery in general rather than to the disclosure of particular trade secrets. *Id.* Addressing the concerns considered by this court in *Gibson-Myers*, the Tenth District explained:

“It is important to bear in mind the underlying rationale for finding an order compelling discovery to be a final, appealable order, which is to prevent the dissemination of protected materials and to avoid the quagmire of being unable to unring the proverbial bell. Neither scenario is present here, because the trial court’s discovery order fully contemplates the imposition of adequate safeguards during the discovery process. While the exact type of safeguards to be imposed and the mechanics of how they will be implemented are not clear, the trial court did indicate the use of protective orders and confidentiality agreements, and we are confident that if additional hearings, in-camera inspections, and the like are warranted, then the trial court will undertake what is necessary to protect the dissemination of proprietary material and trade-secret information.” *Id.* at ¶13.

See, also, *Lambda Research v. Jacobs*, 170 Ohio App.3d 750, 2007-Ohio-309, at ¶14-15 (distinguishing *Dispatch Printing* because, in that case, “[c]entral to the court’s analysis was the fact that safeguards were in place to address the parties’ concerns regarding proprietary information or trade secrets.”) Although not

explicitly stated, therefore, it appears that the Tenth District determined that the order, while related to a provisional remedy, did not satisfy R.C. 2505.02(B)(4)(a).

{¶11} Although the order from which RIS has appealed falls within the definition of a provisional remedy provided by R.C. 2505.02(A)(3), it neither “determines the action with respect to the provisional remedy” nor “prevents a judgment in the action in favor of the appealing party with respect to the provisional remedy” as required by R.C. 2505.02(B)(4)(a). Because RIS’s motion for a protective order sought to prohibit discovery entirely with respect to NIC’s requests for production of documents, the trial court has not been presented with the opportunity to determine whether any particular documents constitute trade secrets. Although the parties seem to agree at this point that the discovery sought by NIC may contain trade secrets, the record indicates that considerable dispute remains about the extent to which that is the case. The trial court’s orders have allowed discovery of a class of documents subject to protection without making a determination with respect to any. The protective orders currently in place preserve RIS’s ability to designate materials as trade secrets while maintaining the parties’ rights to object, whether those materials are produced in hardcopy form or in an electronic medium.

{¶12} In this case the trial court has allowed discovery to proceed subject to general protections while maintaining the parties’ ability to object in the case of specific documents. The order does not determine the action with respect to the

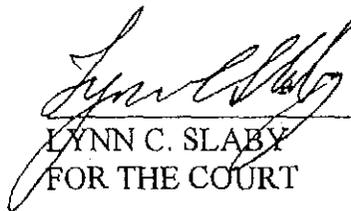
provisional remedy, and the requirements of R.C. 2505.02(B)(4) are not met at this time. Because the order from which RIS has appealed is not a final appealable order within the meaning of R.C. 2505.02, this court does not have jurisdiction to consider this appeal.

Appeal dismissed.

---

Immediately upon the filing hereof, this document shall constitute the journal entry of judgment, and it shall be file stamped by the Clerk of the Court of Appeals at which time the period for review shall begin to run. App.R. 22(E). The Clerk of the Court of Appeals is instructed to mail a notice of entry of this judgment to the parties and to make a notation of the mailing in the docket, pursuant to App.R. 30.

Costs taxed to Appellants.



---

LYNN C. SLABY  
FOR THE COURT

CARR, P. J.  
WHITMORE, J.  
CONCUR

APPEARANCES:

JOHN H. SCHAEFFER and SUSAN A. BAKER, Attorneys at Law, for Appellants.

TIMOTHY WHITFORD, Attorney at Law, for Appellants.

MARK S. FLOYD, CHRISTOPHER JOHNSON, and TIMOTHY H. LINVILLE, Attorneys at Law, for Appellees.

DANIEL M. HERRIGAN

2007 AUG 27 PM 1:55

IN THE COURT OF COMMON PLEAS /  
SUMMIT COUNTY, OHIO COURTS

NATIONAL INTERSTATE CORP., et al.	)	CASE NO. CV-2007-03-1684
	)	
Plaintiff,	)	JUDGE JUDITH L. HUNTER
	)	
vs.	)	
	)	
ANDREW WEST, et al.	)	
	)	
Defendants.	)	
	)	

**PROTECTIVE ORDER GOVERNING  
IMAGING, INSPECTION OF COMPUTERS AND ELECTRONIC DEVICES,  
PROTECTION OF CONFIDENTIAL AND PRIVILEGED INFORMATION  
AND PRESERVATION OF PRIVILEGE IN THE EVENT OF INADVERTENT  
PRODUCTION OF PRIVILEGED MATERIAL**

**IT IS HEREBY ORDERED** that, pursuant to Rule 26 of the Ohio Rules of Civil Procedure, the following procedure shall govern the inspection of all parties' and non-parties' computers during these proceedings.

**A. CREATING CLONES OF THE HARD DRIVES IN RELEVANT COMPUTERS**

1. The producing party will make all computers and other electronic communication devices (hereinafter the "Relevant Computers") that he/she/it owns, controls, and/or possesses available within thirty (30) days of this Order at a mutually convenient date and time to allow Vestige Forensics, Inc. (hereinafter "Vestige") to make a forensic copy of each of the hard drives installed in each of the Relevant Computers.
2. There is resident on each of the Relevant Computers data that is relevant to the claims or defenses of the parties and/or which may lead to the discovery of admissible evidence. All relevant data can be categorized as Content and/or Artifact data. Content data includes all data generated by a human, while Artifact data is generated by a computer.
3. Vestige shall create on its evidentiary hard drives a forensic byte-by-byte exact

image clone (hereinafter "Clone") of each of the hard drives installed or connected to the Relevant Computers (hereinafter "Source Hard Drives").

4. As Vestige creates each Clone, Vestige will also create and embed a "digital fingerprint" (Cyclic Redundancy Check ("CRC") and MD5 algorithm hash) verifying that each Clone is an exact, precise, reliable, mirror image copy of each Source Hard Drive.
5. The producing party's counsel, or counsel's authorized representative, will be allowed to observe the creation of each Clone of each Source Drive onto Vestige's Evidentiary Drive(s).
6. Vestige, and/or its representatives, will perform all work using usual and customary practices and industry standards. Vestige will create each Clone using a combination of one or more of the following techniques, depending upon the circumstances related to each Relevant Computer:
  - a. **Hanging an Evidentiary Drive onto Relevant Computers:**
    - i. Each of the Relevant Computers will be turned off. Special computers, such as servers, will be shut down by the producing party's personnel, using normal shut-down procedures.
    - ii. Each Relevant Computer case will be opened and the internal configuration of the computer noted.
    - iii. Vestige will attach a sanitized evidentiary hard drive (provided by Vestige) to each of the Relevant Computers. The evidentiary hard drive will be attached to a ribbon connecting the evidentiary hard drive to the hard drive controller on the motherboard of each Relevant Computer.
    - iv. Once the evidentiary hard drive is attached, a floppy disk (and/or CD where applicable) will be inserted into each of the Relevant Computers. A Disk Operating System ("DOS") version of the forensic acquisition software is written on the floppy disk or CD.
    - v. Each Relevant Computer will be turned on and booted up to DOS. This prevents any changes being made to the hard drive.
    - vi. The forensic acquisition software will be launched, and a forensic Clone of the Relevant Computer's hard drive will be created onto

the evidentiary hard drive.

- vii. The evidentiary hard drive will be verified.
- viii. The Basic Input and Output System ("BIOS") clock accuracy will be noted.
- ix. Each Relevant Computer will be turned off.

**b. Removing Relevant Computer Hard Drives, Attaching Write Protection And Making Copy:**

- i. Each Relevant Computer will be turned off. Special computers, such as servers, will be shut down by the producing party using normal shut down procedure.
- ii. Each Relevant Computer case will be opened and the internal configuration of the computer noted.
- iii. Each Relevant Computer hard drive will be removed from its case, and a write protection device attached to the Relevant Computer hard drive. The write protection device prevents any data from being written to the Relevant Computer hard drive and prevents any changes from being made to any data on the Relevant Computer hard drive.
- iv. The write-protected Relevant Computer hard drive will be connected to a Vestige field computer containing one or more evidentiary hard drives.
- v. The Vestige field computer will be booted up and the forensic acquisition software will be launched. A Clone of the Relevant Computer hard drive will then be made onto the Vestige evidentiary hard drive.
- vi. The evidentiary hard drive will be verified.
- vii. The Vestige field computer will be turned off, and the write protected Relevant Computer hard drive will be returned to its case.
- viii. The Relevant Computer will be turned on and the BIOS clock accuracy will be noted.

- c. **Cable Acquisition Across Network Card or Parallel Port**
  - i. Relevant Computers will be connected to a Vestige Field Computer via a crossover network cable or a parallel port lap-link cable.
  - ii. Each Relevant Computer will be booted to DOS and placed into server mode.
  - iii. A Clone of each computer will be created on an evidentiary drive provided by Vestige in a manner similar to that above.
- d. **Customized Creation of Clone**

In exceptional circumstances, such as the inability to shut down the Relevant Computer, Vestige will customize the creation of the Clone(s) so as to create a Clone with embedded digital fingerprints and without disrupting the use of the Relevant Computer. These situations ought to be very rare, because almost all computer systems require downtime for many reasons, such as maintenance; and this downtime ought to be sufficient to create a Clone. If a customized method is used to create a Clone, the time to create the Clone may be significantly greater than other methods due to limitations in bandwidth, access times for devices, or other considerations.

**B. EXTRACTING RELEVANT CONTENT, AND IDENTIFYING AND ANALYZING RELEVANT ARTIFACTS**

- 1. Vestige will create a Computer Analysis Team whose members will be responsible for the identification and extraction of relevant Content from the Clone(s) and for the identification and interpretation of relevant Artifacts. The names and curriculum vitae of each member of the Team will be made available to counsel upon request.
- 2. No Vestige personnel will "browse" the Clone(s), hoping to find relevant Content and/or Artifacts. One or more members of The Computer Analysis Team will perform the following analytic functions:
  - a. Configure and/or use a variety of specialized software tools to simultaneously search all areas of each Clone, including in-use space (allocated areas), slack space and unused space (unallocated areas), to

- identify Content and/or Artifacts relating to issues in this lawsuit;
- b. Extract, compile and parse Relevant Content; and
  - c. Extract and analyze Relevant Artifacts.
3. The analysis of the Clones will take place at Vestige. Since the Clones can be made in the presence of the producing party's counsel, and subsequently verified via the MD5 hash checksum, the presence of the producing party's counsel during the analysis of the Clones is unnecessary. Since much of the analysis and searching of Clone(s) can be carried out in an automated, unattended fashion, if the producing party's counsel insists on observing the analysis, the producing party shall pay Vestige's fees for the time spent attending to the analysis of the Clone.
4. Vestige provides protocols and procedures to protect content and to assist in the production of relevant Content and Artifacts. Vestige specifically agrees to abide by the terms of any protocol or procedures in this case.
5. Vestige shall report the results of its analysis in the following manner:
- a. From time to time, Vestige shall prepare the following types of reports: a Report of Relevant Content, an Abstract of Select Provisions of the Report of Relevant Content (hereinafter the "Abstract"), and a Report of Relevant Artifacts.
    - i. Relevant Content. The Report of Relevant Content will include the results of Vestige's search and analysis of Relevant Content, including in native format (or in the format(s) as agreed upon), electronic copies of all relevant content data. Vestige will extract the metadata from the Relevant Content where available, and will create one or more spreadsheets identifying all Relevant Content by its MD5 value. Vestige will link the MD5 identifier in the spreadsheet(s) with the file containing the content so that a user can review the content from within the spreadsheet
    - ii. Abstract. The Abstract shall be limited to a statement of the number of pages in the Report of Relevant Content, the procedures and processes used by Vestige to complete its analysis of Relevant Content and Artifacts, the number of pieces of Relevant Content data included in the Report of Relevant Content, and authentication information

related to the Source Hard Drives and Clones.

- iii. Artifacts. The Report of Relevant Artifacts shall include Vestige's opinion and all artifacts related to the manner in which Relevant Computers were used, the state of the data resident upon the Relevant Computers (including certification of completeness of data and integrity of data), and any other Relevant Computer usage issue.
- b. Vestige shall file the Abstract and Report of Relevant Artifacts by serving a copy on all parties. Vestige shall file the Report of Relevant Content by serving a copy on counsel for producing party only. Upon request of the parties, Vestige shall file with the Court a copy of the Abstract and the Report of Relevant Artifacts, and shall file under seal the Report of Relevant Content.
- c. Vestige shall simultaneously serve a copy of the Abstract and a copy of the Report of Relevant Artifacts upon counsel for the producing party and counsel for the requesting party.
- d. Within ten (10) business days of receiving an electronic copy of the Report of Relevant Content with Appendices and Exhibits, counsel for producing party will redact the Report for privilege, prepare a privilege log identifying the items in the Report of Relevant Content that counsel has redacted and the grounds therefore, and serve a copy of the Redacted Report of Relevant Content on counsel for requesting party.
- e. The Redacted Report of Relevant Content will be served on counsel for the requesting party in the same electronic format as it was created by Vestige, except redacted electronic copies of relevant data will be produced in PDF or some other acceptable format. The purpose of this provision is to cause all non-redacted, relevant data to be produced in native format with metadata attached to the electronic files, and all redacted relevant data to be produced in PDF, TIFF, or some other format that protects the redaction from being recovered.
- f. Service of the Abstract and Report of Relevant Artifacts shall be deemed complete for each when Vestige places into the United States mail one or more CD-Rom or DVD containing an electronic copy of the Abstract and the Report of Relevant

Artifacts, including all Appendices and Exhibits.

- g. In some cases, circumstances may require that Vestige create and produce Relevant Content and Artifacts as they are identified, extracted and analyzed. In this event, Vestige shall prepare an index of items included in each "rolling" production of Relevant Content and Relevant Artifacts (hereinafter the "Rolling Index of Content and Artifacts"). The Rolling Index of Content and Artifacts shall append the items included in each rolling production, so that the Index continues to expand with each "rolling" production.
  - h. Each Rolling Production of Relevant Content shall be served only upon counsel for the producing party, who shall redact the Content for privilege and prepare a privilege log in accordance with Paragraph B(4)(a)(d) above, and serve the Redacted Relevant Content in accordance with paragraph B(4)(a)(c) above.
  - i. Each Rolling Production of Relevant Artifacts shall be served simultaneously by Vestige on counsel for the producing party and counsel for the requesting party.
5. Any information contained on Clones that is not reported by Vestige shall be considered Confidential Information and subject to the provisions of this Order. Any data reported by Vestige that is claimed by producing party's counsel to be subject to attorney-client privilege shall be treated as Confidential Information. Vestige and its representatives, agree not to reveal to, or discuss with requesting party's Counsel any Confidential Information absent a modification of this Protective Order or Court Order. Vestige agrees to subject itself to the jurisdiction of the Court and the parties agree that Vestige has standing to request Court intervention to protect Vestige's economic, reputation, and/or legal interests in this matter.
6. The inadvertent or intentional disclosure by Vestige or any representative of Vestige of Confidential Information shall not be deemed a waiver in whole or in part of the producing party's claim of confidentiality or protection under this Order, either as to specific information disclosed or as to any other information relating thereto or on the same or related subject matter. Counsel for the parties, and the producing party's personal counsel, shall, in any event, upon discovery of inadvertent error, cooperate to restore the confidentiality and

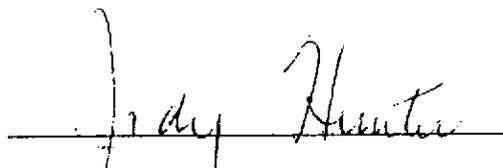
protection of the Confidential Information.

- 7. Nothing in this Order shall prevent the parties from using relevant, non-confidential information derived from the inspection of any Relevant Computer in connection with the trial, hearings, depositions, motions, memoranda or other proceedings in this action. Nor shall this Order prevent the parties from obtaining from Vestige by way of testimony or affidavit, explanations of the process, procedure, or results used or obtained by Vestige.

**C. PRIVILEGE REVIEW AND PRODUCTION**

The Court is aware that the producing party must conduct a privilege review of the Relevant Data prior to producing same to the requesting party. In the event that the producing party concludes that, due to the volume of Relevant Data, it cannot complete the privilege review of all Relevant Data within ten business days, the producing party may, upon good cause shown, request an extension of time to complete the review and to identify any privileged matters. However, the Court may compel the production of all Relevant Data with less than full privilege review and find that such a production does not waive the claim of privilege for any material.

**IT IS SO ORDERED**

  
 \_\_\_\_\_  
**JUDGE JUDITH HUNTER**

DANIEL M. HERRIGAN

2007 AUG 27 PM 1:55

IN THE COURT OF COMMON PLEAS  
SUMMIT COUNTY, OHIO  
CLERK OF COURTS

NATIONAL INTERSTATE CORP.,	)	CASE NO. CV-2007-03-1684
	)	
Plaintiff,	)	JUDGE JUDITH L. HUNTER
	)	
vs.	)	
	)	<b>ORDER REGARDING PROTECTION</b>
ANDREW WEST, et al.	)	<b>OF CONFIDENTIAL INFORMATION</b>
	)	
Defendants.	)	

Pursuant to Rule 26(C) of the Ohio Rules of Civil Procedure, upon stipulation of all the parties and for good cause shown,

IT IS HEREBY ORDERED THAT:

1. (a) "Confidential Information" shall mean any information, whether oral or written, produced during the course of discovery by a party or non-party subpoenaed in connection with this action (the "producing party") that the producing party reasonably and in good faith believes would disclose confidential, proprietary, personal information, trade secret or other sensitive business or technical information. The producing party shall designate Confidential Information as "Confidential: Subject to Protective Order" or "Confidential" either (i) before production or (ii) after the party to whom production is made (the "receiving party") has inspected the documents produced for inspection and copying and has made an election as to the documents which that party will copy for retention. Documents produced in this action may be designated by any party or parties by marking the first page of the document in this manner. Documents unintentionally produced without such designation may be retroactively designated as Confidential

Information by written notice of the producing party and shall be treated as Confidential Information from the date of such notice.

(b) Any party may, in good faith, designate as "ATTORNEY'S EYES ONLY" any Confidential Information which, if disclosed, could significantly and irreparably prejudice its business dealings or interests with customers or potential customers, or intrude upon the privacy of any nonparty (this subset of Confidential Information shall be referred to as "Attorney's Eyes Only Material"). In the event of such a designation, only attorneys of record and designated experts may have access to the Attorney's Eyes Only Material. Attorney's Eyes Only Material shall not be disclosed under any circumstances to anyone including the parties, their current employees, in-house counsel, or officers without first obtaining the written approval of the producing party making the designation. Any expert to whom Attorney's Eyes Only Material is provided, as a condition of receiving such material, shall fully abide by all terms of this Order and prior to any disclosure is made to the expert, shall execute and provide to producing party, an Acknowledgment in the form attached hereto as Exhibit A. Attorney's Eyes Only Material may, however, be used in the course of litigation— including but not limited to depositions, pleadings, hearings, or trial of this matter— subject to the limitations contained in paragraph 6.

2. All Confidential Information produced or exchanged in the course of this litigation shall be used solely for the purpose of preparation, trial, or any appeal of this litigation and for no other purpose whatsoever, and shall not be disclosed to any person or used for any purpose except in accordance with the terms of this Order.

3. All Confidential Information shall be maintained under strict confidence by trial counsel for the parties and shall not be disclosed or made available by the receiving party to persons other than "Qualified Persons." Qualified Persons as used herein means:

- (a) members or employees of trial counsel's firm who are engaged in the preparation for any hearing or trial in this action;
- (b) court reporters in the performance of their official duties;
- (c) this Court, including Court personnel;
- (d) with respect to a particular item of information or document, persons, including parties, who prepared or assisted in the preparation of that item or document, or to whom the item or document or a copy thereof was addressed or delivered, but only to the extent such disclosure and any use of the information is for the conduct of this action;
- (e) expert witnesses or consultants retained solely for purposes of this litigation provided that such witness or consultant is not otherwise affiliated with or employed by a party and who have executed an Acknowledgment;
- (f) the parties, including current employees, officers and directors of corporate parties (Attorney's Eyes Only Material shall not be disclosed except as provided for in paragraph 1(b)); and
- (g) any other person upon the prior written consent of the producing party or upon order by the Court.

4. Other than those persons identified in paragraphs 3(a)-(d) and (f), any person to whom Confidential Information is disclosed shall, prior to disclosure, be required by the disclosing party to read this Order and agree in writing to be bound by its terms and conditions and to subject himself to the jurisdiction of this Court for the purpose of contempt proceedings if he violates this Order. Such person shall execute an Acknowledgment in the form attached to this Order as Exhibit "A", prior to being given access to Confidential Information. Counsel for the party disclosing the Confidential Information shall maintain these written certifications, and they shall be available to

opposing counsel for inspection upon termination of the litigation. The provisions of this paragraph shall survive final termination of this action.

5. As used in this Order, "trial counsel" refers exclusively to counsel who have entered an appearance in this action on behalf of one or more of the parties.

6. Subject to the restrictions contained herein, nothing in this Order shall prevent a party from using at trial or any hearing or during a deposition, or in connection with briefs or other papers filed with the Court, any Confidential Information, except that any such use shall not expand the persons to whom Confidential Information may be disclosed pursuant to this Order. In the event a party wishes to use Confidential Information in any papers filed with the Court or files deposition transcripts containing Confidential Information with the Court, such papers and transcripts shall be filed under seal with the Court.

If Confidential Information and/or Confidential "For Attorneys' Eyes only" information is used during a deposition, that portion of the deposition will be conducted without the presence of any person or party, except the witness, not eligible to receive a disclosure of the information under paragraphs 2 or 3, as the case may be, of this Order, and the transcript will be marked pursuant to this Order. Prior to the use of Confidential Information at a hearing, the parties will discuss with the Court appropriate procedures to prevent disclosure of Confidential Information. Confidential Information shall not become a part of the public record except upon the written consent of the producing party or unless permitted by this Court, after the producing party has had an opportunity to present its arguments regarding confidentiality to the Court.

7. Depositions.

(a) Documents containing Confidential Information may be used by any party at any deposition in this action provided that the terms of this Order, including the restrictions on who may

have access to such information, as set forth in paragraphs 2 and 3, and the restrictions of paragraph 6 shall apply.

(b) Oral deposition testimony may be designated as Confidential Information by making an appropriate statement on the record at the time of the deposition. Any party may also designate information disclosed at a deposition as Confidential Information by identifying, within thirty (30) days following receipt by counsel of a copy of the transcript, the specific pages and lines of the transcript that are so designated and notifying the other parties in writing of such designation. Irrespective of whether any designation is made at the time a deposition is taken, the entire transcript of each such deposition shall be treated as Confidential Information during the thirty (30)-day period. Unless otherwise designated as specified in this Order, the transcript shall not be treated as Confidential Information after the stated thirty (30)-day period.

(c) Prior to the disclosure of Confidential Information at any deposition, the reporter recording the same shall be furnished with a copy of this Order by the party taking the deposition and shall be informed that testimony, exhibits and other Confidential Information may be disclosed only in accordance with the terms of the Order. When a transcript of the testimony is prepared, the reporter shall conspicuously mark each page on which Confidential Information appears with an appropriate legend signifying its protected status and shall place the following legend on the cover of any transcript containing Confidential Information: "This transcript contains Confidential Information subject to a Protective Order of the Court." The reporter shall treat the transcript in accordance with the terms of this Order.

8. Trial.

Any party may introduce evidence at trial that is designated Confidential Information provided that the party seeking to introduce the Confidential Information has first given the

producing party written notice at least thirty (30) days prior to trial, or sooner if there is a Court order requiring identification of exhibits earlier, of its intent to introduce Confidential Information at trial. If any party wishes to prevent the ordinary and public use at trial of anything produced as Confidential Information under this Order, or ask that such information be kept under seal or otherwise confidential in any way, that party must raise the issue with opposing counsel and the Court at least 15 days in advance of the scheduled trial date. If the parties cannot agree upon whether to use the Confidential Information at trial, the Court shall decide whether the Confidential Information can be used at trial.

9. Any person receiving Confidential Information under the terms of this Order shall make no use of the information except for purposes of the preparation for a hearing, trial, appeal or settlement of this action. No person shall make copies, extracts, or summaries of Confidential Information except under the supervision of counsel when, in the judgment of counsel, such copies or other papers are necessary for the conduct or settlement of the action. Each such copy or other paper shall be conspicuously marked with an appropriate legend signifying its status as Confidential Information. Counsel and all other persons to whom Confidential Information is disclosed pursuant to paragraphs 2 or 3, as the case may be, of this Order shall take reasonable and appropriate precautions to avoid loss or inadvertent disclosure of such materials.

10. Nothing contained in this Order shall be construed as an admission by any party that any document or information designated as "Confidential Information" is in fact confidential, proprietary or a trade secret or as a waiver by either party of its right to object to the subject matter of any discovery request made in this action. The execution of this Order shall not be construed as an agreement by either party to produce any documents, supply any information, or permit entry upon land under Ohio R. Civ. P. 34, and shall not constitute an admission that any evidence,

including documents, which may exist is relevant in any way to the issues raised in this action or a waiver of any privilege with respect thereto.

11. This Order shall be without prejudice to the right of any party to bring before this Court at any time the question of whether any particular information is discoverable, relevant or admissible to any issue in this case.

12. Designation by a party of information or a document as Confidential Information shall have no evidentiary significance and may not be used at a hearing or at trial for any purpose. A party's failure to object to a producing party's designation shall likewise have no evidentiary significance and shall not constitute an admission that the information is confidential.

13. If a receiving party disagrees at any time during this action with the producing party's designation, such party shall notify the producing party in writing of its disagreement with the designation. The parties shall first try to resolve the dispute in good faith on an informal basis. If the dispute cannot be resolved informally, the party challenging the designation may request appropriate relief from the Court pursuant to Ohio R. Civ. P. 37. The burden of proving that the information has been properly designated as Confidential Information shall be on the producing party. The parties may provide for exceptions to this Order by written stipulation and any party may seek an order of the Court modifying this Order.

14. Nothing in this Order shall bar or otherwise restrict any attorney from rendering advice to his or her client with respect to this action and, in the course thereof, from referring to or relying generally upon his or her examination of Confidential Information or Attorney's Eyes Only Material. However, in rendering any such advice or in otherwise communicating with his or her client, the attorney shall not disclose the contents

or source of any Attorney's Eyes Only Material in any manner contrary to the terms of this Order.

15. Upon final termination of this action, whether by settlement, judgment or appeal, each party shall within sixty (60) days assemble and return to the opposing party, or at the producing person's option request that receiving party certify the destruction of, all documentary material or memoranda embodying information designated "Confidential Information" including all copies of such memoranda or documentary material which may have been made.

16. No later than thirty (30) days after the final termination of this action, counsel for each party shall contact the Court if they wish to retain any documents designated as Confidential Information. Otherwise, the Court will thereafter destroy any unclaimed documents so designated.

17. This Order may be extended to additional parties or nonparties by written consent of all of the parties that are signatories to this agreement.

18. All documents, materials and information previously withheld as confidential and/or under claim of trade secret protection shall be produced to the requesting party within thirty (30) days of this Order.

19. The Court will address issues surrounding electronic discovery, including the protocol for and timing of imaging, inspection of computers and electronic devices, protection of confidential and privileged information and preservation of privilege in the event of inadvertent production of privileged material in a separate protective order.

IT IS SO ORDERED.

Dated: 5/27/07

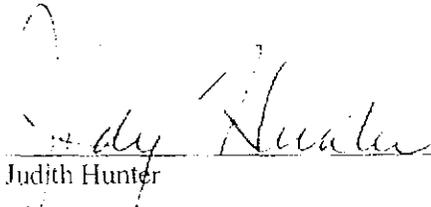
  
\_\_\_\_\_  
Judge Judith Hunter

EXHIBIT A

IN THE COURT OF COMMON PLEAS  
SUMMIT COUNTY, OHIO

NATIONAL INTERSTATE CORP.,	)	CASE NO. CV-2007-03-1684
	)	
Plaintiff,	)	JUDGE JUDITH L. HUNTER
	)	
vs.	)	
	)	
ANDREW WEST, et al.	)	
	)	
Defendants.	)	ACKNOWLEDGMENT

\_\_\_\_\_ hereby acknowledges and agrees that s/he has been provided with a copy of the Stipulated Protective Order entered in the above captioned action; s/he has read the Order; s/he agrees to be bound by its terms; and s/he subjects himself/herself to jurisdiction of the Court of Common Pleas, Summit County, Ohio, for purposes of any action to enforce the terms of the Order. I understand that any violation of the Stipulated Protective Order by me or anyone acting under my direction may subject me to sanctions imposed by the Court, including, but not limited to, penalties for contempt of court.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature

11310323.1