NOT PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

_____

No. 09-4208

_____

JOSEPH OAT HOLDINGS, INC.;
BIOTHANE CORPORATION; ROBERT SAX;
MICHAEL HOLTZ; GRAIG ROSENBERGER;
MARTIN KAPLAN; RONALD KAPLAN; JOHN MURPHY;
RCM BIOTHANE, LLC, a nominal plaintiff,
Appellants

v.

RCM DIGESTERS, INC.;
MARK MOSER

_____

On Appeal from the United States District Court
for the District of New Jersey
D.C. Civil Action No. 06-cv-4449
(Honorable Noel L. Hillman)

_____

Argued September 15, 2010

Before: SCIRICA, RENDELL and FISHER, *Circuit Judges*.

(Filed: December 13, 2010)

R. JAMES KRAVITZ, ESQUIRE (ARGUED)
MUKTI N. PATEL, ESQUIRE
Fox Rothschild
Princeton Pike Corporate Center, Building 3
997 Lenox Drive
Lawrenceville, New Jersey 08648
Attorneys for Appellants

JAMES C. DUDA, ESQUIRE (ARGUED)
ERIC D. BEAL, ESQUIRE
Buckley, Richardson and Gilinas
1500 Main Street, Suite 2700
Springfield, Massachusetts 01115

WILLIAM J. DESANTIS, ESQUIRE
Ballard Spahr
210 Lake Drive East, Suite 200
Cherry Hill, New Jersey 08002

JOSEPH H. KENNEY, ESQUIRE
Ballard Spahr
Plaza 1000, Suite 500
Main Street
Voorhees, New Jersey 08043
Attorneys for Appellees

---

OPINION OF THE COURT

---

SCIRICA, *Circuit Judge*.

This appeal involves an overlap between substantive claims under state and federal anti-hacking laws and alleged electronic discovery misconduct. The underlying suit arises out of a failed joint venture and subsequent copying of electronic files by one of the parties through a joint computer network that connected the parties to the joint venture. Following initiation of this action, appellants, individuals and corporations associated with one party to the joint venture, Biothane Corporation, accessed a server used by the joint venture, and copied files. In addition to seeking discovery sanctions for obtaining the files allegedly outside the discovery methods sanctioned by the Federal Rules of Civil Procedure, appellees, Mark Moser and his corporation, RCM Digesters,

Inc., the counterpart in the joint venture, amended their counterclaims to sue under state and federal anti-hacking laws for unauthorized access to the server.

The District Court granted summary judgment in favor of Moser and RCM Digesters, finding Biothane liable under state anti-hacking laws and enjoining them from retaining or using copies of the data. Because it remains disputed whether Biothane and its employees, in fact, had authorization to access the server, we will vacate the grant of summary judgment and remand for further proceedings consistent with our opinion.

I.

Biothane Corporation, a wholly owned subsidiary of Joseph Oat Holdings, Inc., ("JOHI"), is a multinational corporation specializing in the biological treatment of wastewater. Mark Moser is the founding stockholder of RCM Digesters, Inc., a business that develops anaerobic digester systems, which are containers of bacteria that break down organic wastes and produce methane. On February 17, 2005,[1] Biothane and RCM Digesters created a joint venture, RCM Biothane; JOHI owned eighty percent and Moser owned twenty percent. The appellants[2] are JOHI, Biothane, and individual plaintiffs[3]

[1] The Certificate of Formation is dated February 17, 2005.

[2] Appellants were the plaintiffs/counterclaim-defendants below. Additional counterclaim defendants are Martin Kaplan, Ronald Kaplan, Michael Holtz, and Graig Rosenberger, who were all employees or board members of JOHI or Biothane. Before the order at issue here was made, the parties voluntarily dismissed the Kaplans, Holtz and Rosenberger as defendants for the claims involved in this appeal.

[3] The individual plaintiffs were JOHI's designees to the board of managers. Some were also executives of Biothane. All had financial interests in Biothane, JOHI, or both.

Robert Sax,[4] and John Murphy, who were members of RCM Biothane's board of managers. RCM Biothane is a nominal plaintiff, as its dissolution was approved by the board of managers. We refer to appellants as the Biothane parties.

A.

Disputes between the parties resulted in a short-lived business arrangement. Less than two years after the joint venture began, the parties entered into a separation agreement dated August 7, 2006.

On August 7, 2006, at a board of managers' meeting to discuss dissolution of RCM Biothane, the parties signed the separation agreement, which specifies, "[a]ll documents received by Purchaser and its subsidiaries as part of the asset purchase agreement are to be expeditiously returned to Moser, or in the case of electronic files, erased" and "[a]ll documents and electronic files generated in the pursuit of sales related to manure digestion shall be expeditiously provided to Moser." It also states, "Biothane will cooperate fully with Moser to facilitate his ability to carry on his business going forward including the expeditious restoration of his computer system independent of Biothane's computer system and modification of the website to reflect and communicate with RCM Digesters."

A prior agreement does not appear to give Moser the right to RCM Biothane's assets. The Limited Liability Company Agreement of RCM Biothane, LLC, specifies that all rights of management are exclusively vested in the board of managers and only

[4] President of Biothane.

RCM Biothane or a designee of the board of managers shall have any rights, title, or interest in RCM Biothane property "of any kind."

The Biothane parties claim that Moser repudiated the separation agreement shortly after it was reached. Emails indicate that Moser repeatedly told employees of Biothane that he viewed the agreement as void or incomplete. The Biothane parties claim Moser continued to operate RCM Biothane well after the separation agreement was signed.

B.

On September 20, 2006, the Biothane parties commenced the present action alleging trademark infringement in violation of 15 U.S.C. § 1125(a), unfair competition, breach of contract, breach of the covenant of good faith and fair dealing, breach of fiduciary duties, and fraud. The defendants, Moser and RCM Digesters, filed a counterclaim and third party complaint alleging fraud, breach of contract, violation of the Anticybersquatting Act, 15 U.S.C § 1125(d), trademark infringement in violation of 15 U.S.C. § 1125(a), misappropriation of trade secrets, and unjust enrichment.

On October 11, 2006, James C. Duda, attorney for the Moser and RCM Biothane, sent a "litigation hold" letter to R. James Kravitz, attorney for the Biothane parties. The relevant portion of the letter states:

> As you know, the laws and rules prohibiting destruction of evidence apply to electronic data with the same force as they apply to other kinds of evidence. This letter is to remind you to ensure that your clients, [the Biothane parties], have been mindful of and have taken proactive steps to ensure preservation of relevant electronic evidence associated with this matter pending its resolution. Your clients' preservation obligations include, at a minimum, the following:

- Identifying those individuals and entities currently or formerly associated with JOHI, Biothane Corporation, and/or RCM Biothane, including but not limited to [specified individuals], who potentially possess or control, or possessed or controlled, relevant recorded information, whether in electronic or hard-copy form, and taking steps to ensure that **all** recorded information potentially relevant to JOHI's claims and defenses and any potential counterclaims or defenses that [the RCM parties] might raise, wherever that material may be found, are identified and preserved pending resolution of this matter . . . .

(emphasis in original). On October 20, 2006, Duda sent another letter reminding Biothane to preserve "all electronic data pertaining to any and all activities of RCM Biothane LLC, RCM Digesters, Inc. and Mark Moser."

According to the Moser's and RCM Digester's expert, Timothy O'Shea, the computer networks of JOHI and RCM Biothane were connected in June of 2005 via a virtual private network (VPN). The purpose of a VPN is to "create a seamless unbroken connection between different locations." Data servers were located in Camden, New Jersey, the site of the JOHI network, and Oakland, California, the site of the RCM Biothane network. The server in Oakland was called the "cube" server. The only administrators of the VPN were Biothane employees in Camden. Moser did not have administrative privileges. O'Shea states that "parameters of authorized access, such as from what PC or even which office location, time or day of the week, to what the user can do with the files, [could] all be controlled by the admin in the Camden office." O'Shea concludes the lack of anyone at the Oakland Site with administrative power over that location departed from usual practice in the IT field. The report also states that:

It has long been the common practice of IT administrators to maintain and

> organize the users on the network while having access to the data without resorting to looking through that data to collect information, copy files, or delete or manipulate data, either for the administrators' own use or the use of others, except by way of company policy in which all users know of the same policy. . . . Absent authorization from RCM Digesters, the administrator for content of its server in the Oakland office should not have been accessing, copying, or destroying files.

Mark Moser states he never authorized the Biothane parties to access and copy files from the cube server.

Stephen Murphy, IT manager at Biothane, claimed that Biothane had access to the documents on the server and Moser knowingly placed all documents on the Biothane/JOHI computer system. An email from Chris Soltys, who administered Biothane's network, indicates that Biothane's position was that the cube server was under Biothane's IT policy until it was disconnected from the VPN. Thus, in the view of Biothane's employees, only they, and not Moser, had ultimate control of the server and the files on it.

In October 2006, Biothane copied the files residing on the Oakland cube server. In emails, Biothane personnel referred to this as the "information copy project." Several internal Biothane emails from October 11, 2006, refer to the need to back up files on the cube server to preserve access to them. Biothane employees asked that it be done "under the radar." A desktop "shortcut" to allow employees of JOHI and Biothane to easily access the copied data was created on some computers. At his deposition, Jay Murphy, Vice President of Biothane, stated that he ordered the copying of the data on the cube server pursuant to the directive in James Duda's litigation hold letter. Jay Murphy

considered Biothane to have access to and to own the files because they were on the JOHI computer system via the VPN. He stated that Biothane had previously presented Moser with a detailed plan to disconnect the networks, which Moser ignored. Murphy stated he was concerned, after a conversation with his IT manager, Chris Soltys, that, if Moser disconnected the VPN on his own, the files and computer system would be damaged. Accordingly, he ordered the copying to preserve the files. Biothane employees also changed administrative passwords on the server and deleted backup disks.

On November 14, 2007, Moser and RCM Digesters moved to amend the counterclaim to add counts alleging violations of California, New Jersey, and Federal anti-hacking laws arising from the Biothane parties' unauthorized access of the computer server. The counts at issue here[5] include: Count 19, violation of California's Computer Data Access and Fraud Act, Cal. Penal Code § 502; Count 20, violation of a similar New Jersey statute, N.J. Stat. Ann. § 2A:38A-1; and Count 21, violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200. On March 27, 2008, the District Court granted leave to amend.

On June 27, 2008, a Magistrate Judge issued an opinion and order on Moser's and RCM Digester's motion for sanctions for copying files from the cube server. The court

[5] Summary judgment was not granted in the order being appealed from on other counts, a determination from which Moser and RCM Digesters have not cross-appealed. These are: Count 18, violation of the Federal Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; Count 22, conversion; Count 23, civil conspiracy; and Count 24, aiding and abetting.

found there was "no question that [the Biothane parties'] actions were willful in the sense that [they] deliberately copied [Moser's and RCM Digester's] documents" but stated "the Court does not find that plaintiffs acted in flagrant bad faith." The court went on to reject the Biothane parties' proffered explanation of acting pursuant to the litigation hold letter, but stated "it appears to this Court that plaintiffs accessed defendants' computer to preserve business documents, not for the purpose of gaining an advantage in this litigation." Furthermore, the court found "plaintiffs could believe they had a justifiable and legal right to access defendants' documents." The Magistrate Judge imposed a sanction of paying the "reasonable out-of-pocket costs defendants incurred, not attorney's fees, to take the discovery specifically directed to finding out what documents were copied from their computer system."

On March 31, 2009, the District Court denied summary judgment for claims relating to the separation agreement. The District Court found "material issues of disputed fact remain as to the validity of the separation agreement" but that "neither party disputes that they wanted to dissolve the business relationship and execute a writing to memorialize all the attendant details." It "is disputed that the Separation Agreement is that writing [memorializing the details]" as the document may not have been "complete enough to constitute a binding agreement." In regard to the purported date of separation of August 7, 2006, the District Court stated:

> [T]he one undisputed fact is that the parties wanted a business divorce, and on August 7, 2006, they discussed the details of that divorce. The fact that Moser still continued to operate RCM Biothane after August 7, 2006, despite the language in

> the Separation Agreement that "RCM Biothane is dissolved," demonstrates that in practical effect, even if the Separation Agreement were valid, time was necessary to wind down the affairs of RCM Biothane.

The District Court could not determine the validity or the terms of the separation agreement at the summary judgment stage.

In an order and opinion of October 14, 2009 giving rise to this appeal, the District Court addressed the cross-motions for summary judgment involving the RCM parties' counts alleging violation of state and federal anti-hacking laws. The District Court separated the documents copied into two categories—those created before August 7, 2006 and those created after August 7, 2006—because "the documents plaintiff copied from defendants' computer server that were created after the August 7, 2006 business divorce are undisputedly the sole property of defendants."

The District Court granted summary judgment in favor of the RCM parties and against the remaining Biothane Parties, on Count 19, California's Computer Data Access and Fraud Act, Cal. Penal. Code § 503(c).[6] The District Court stated the RCM parties provided evidence: (1) "that plaintiffs called their actions the 'Information Copy Project' and that they intended to keep it a secret, which they did for over a year," (2) "that computer desktop 'shortcuts' were placed on the computers of the individual plaintiffs

[6] Section 502 provides:

> In addition to any other civil remedy available, the owner or lessee of the computer, computer system, computer network, computer program, or data who suffers damage or loss by reason of a violation of any of the provisions of subdivision (c) may bring a civil action against the violator for compensatory damages and injunctive relief or other equitable relief.

Cal. Penal Code. § 502(e)(1).

and other Biothane employees so they would have quick access to the copied files," and (3) that "at the time the plaintiffs accessed the cube server[, the server] had reverted back to the property of RCM Digesters, . . . RCM Biothane, which previously had access to the cube server, was defunct, and . . . plaintiffs had no interest or rights in RCM Digesters." The District Court found Jay Murphy's claim that the documents were preserved for litigation was undercut by the secretive nature of the project and the creation of desktop shortcuts for Biothane employees to access the documents for business purposes. With regard to the claim that access was privileged litigation conduct, the court "found that plaintiffs' clandestine copying of computer files was not conducted purely for litigation, or, more specifically, e-discovery purposes." Lastly, the court found the ownership of the server was not disputed post-August 7, 2006, because there was no genuine issue of material fact as to whether RCM Biothane dissolved on August 7. The District Court did not find it necessary to revise its prior decision that there were genuine issues of material fact regarding the validity of the separation agreement in order to find Moser and RCM Digesters owned the server.

The District Court found Biothane violated five subparts of California Penal Code § 502(c)[7] and granted summary judgment as to liability on Count 19. As the amount of damages was disputed and could not be resolved until trial, the District Court provided

[7] The court partially rejected the RCM parties' argument as to one subpart regarding the alteration or destruction of data. Cal. Penal Code § 502(c)(4). The court found that the Biothane parties could not be liable for the destruction of data on backup disks, as there were no damages caused by the destruction, because the main data files never failed.

injunctive relief requiring the Biothane parties to return any data created post-August 7, 2006 and forbidding the Biothane parties from using the post-dissolution data in any manner.

The District Court also granted summary judgment in favor of the RCM parties on liability and injunctive relief on Count 20, violation of the New Jersey Computer-Related Offense Act, N.J. Stat. Ann. § 2A:38A-2(a), (c), (e). The court found the New Jersey Act mirrored the California Act and therefore granted summary judgment on the same basis.

Finally, the district court granted summary judgment on liability for Count 21, violation of California's Unfair Competition Law (UCL), Cal. Bus. & Prof. Code § 17200. The violation of California Penal Code § 502 and the New Jersey Computer Related Offenses Act constitute the predicate unlawful acts under § 17200, which requires that there be an "unlawful . . . business act or practice." Accordingly, the same facts are material to liability under the three statutes, as the anti-hacking statutes mirror one another, and the UCL claim is dependent on finding liability under the anti-hacking laws.

II.

There is no final order in this case. We have jurisdiction because the interlocutory order on appeal granted an injunction. *See* 28 U.S.C. § 1292(a)(1) (granting jurisdiction to review interlocutory orders "granting . . . injunctions"). As the district court granted an injunction in its summary judgment order, our "review properly extends to matters inextricably bound up with the injunction decision." *DeJohn v. Temple Univ.*, 537 F.3d

301, 313 (3d Cir. 2008) (citation omitted). "While the scope of appellate review under § 1292(a)(1) is confined to the issues necessary to determine the propriety of the interlocutory order itself, interlocutory orders with respect to permanent injunctions provide frequent occasion for review of the merits." *Id.* If "the permanent injunction is premised entirely on the District Court's grant of summary judgment to plaintiff . . ., to resolve the propriety of the permanent injunction, we must determine whether the District Court erred in granting summary judgment." *Doeblers Pa. Hybrids, Inc. v. Doebler*, 442 F.3d 812, 819 (3d Cir. 2006). Because the injunction derives from the underlying finding of liability under the state law anti-hacking statutes, we review the propriety of granting summary judgment on these counts.[8]

The District Court found undisputed material facts establishing whether the Biothane parties violated two states' anti-hacking laws and California's Unfair Competition Law.[9] The common elements to each subsection of California Penal Code §

[8] We have described our review of orders granting summary judgment, as follows:

> We exercise plenary review over a district court's decision granting summary judgment. *See Prowel v. Wise Bus. Forms, Inc.*, 579 F.3d 285, 286 (3d Cir. 2009). Summary judgment is proper "if the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(c). "A motion for summary judgment will not be defeated by 'the mere existence' of some disputed facts, but will be denied when there is a genuine issue of material fact." *Am. Eagle Outfitters v. Lyle & Scott Ltd.*, 584 F.3d 575, 581 (3d Cir. 2009) (citing *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247-48 (1986)). We draw all inferences in a light most favorable to the nonmoving party. *Id.*

*Sheridan v. NGK Metals Corp.*, 609 F.3d 239 (3d Cir. 2010).

[9] Section 502(c) of the California Penal Code states in relevant part:

502(c) are "knowing access" "followed by [specified] unauthorized" actions. *Facebook, Inc. v. ConnectU, LLC*, 489 F. Supp. 2d 1087, 1091 (N.D. Cal. 2007). The New Jersey Computer Related Offenses Act ("NJ CROA"), N.J. Stat. Ann. § 2A:38A-3, parallels § 502 by requiring knowing access and "unauthorized" actions.[10] The violation of § 502

---

> [A]ny person who commits any of the following acts is guilty of a public offense:
>
> (1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.
>
> (2) Knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.
>
> . . .
>
> (4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.
>
> . . .
>
> (6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network in violation of this section.
>
> (7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network . . . .

Cal. Penal Code § 502(c).

[10] The NJ CROA states in relevant part:

> A person or enterprise damaged in business or property as a result of any of the following actions may sue the actor therefor [sic] in the Superior Court and may recover compensatory and punitive damages and the cost of the suit including a reasonable attorney's fee, costs of investigation and litigation:
>
> a. The purposeful or knowing, and unauthorized altering, damaging, taking or destruction of any data, data base, computer program, computer software or computer equipment existing internally or externally to a computer, computer system or computer network;
>
> . . .

and the CROA also served as the predicate "unlawful . . . business practice" needed to show a violation of California's Unfair Competition Law (UCL). Cal. Bus. & Prof. Code § 17200.[11] We will vacate and remand because the court's decision was premised on ownership of the server, and did not address whether Biothane had authorization or permission to access the server—the element required under the state statutes and about which there were genuine issues of material fact.

The focus at summary judgment was on the ownership of the server and the date the joint venture ceased to exist. While ownership of the server may be an important factor in determining whether the Biothane parties acted without authorization or permission, ownership does not necessarily entitle Moser and RCM Digesters to summary judgment. A change in ownership may not be determinative with respect to whether Biothane had permission to access the server.

The record contains evidence that Biothane may have acted with permission.

---

> c. The purposeful or knowing, and unauthorized accessing or attempt to access any computer, computer system or computer network;
> . . .
> e. The purposeful or knowing accessing and reckless altering, damaging, destroying or obtaining of any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network.

N.J. Stat. Ann. § 2A:38A-3(a), (c), (e).

[11] Section 17200 states in its entirety:

> As used in this chapter, unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code.

Cal. Bus. & Prof. Code § 17200.

During the joint venture and while the venture was winding up, employees of Biothane not only had access to the server via the VPN, but also administered the network. Steven Murphy, an IT manager at Biothane, testified at deposition that Biothane considered the server a part of their network and that anything placed on it could be accessed by Biothane employees. The record appears to be silent on whether Moser and RCM Digesters, assuming they owned the server, rescinded any prior authorization to access the server, express or implied.

Furthermore, ownership may still be in dispute. The District Court declined to grant summary judgment as to the validity of the separation agreement because material facts remained in dispute. Because the separation agreement appears to be the only agreement that would give Moser and RCM Digesters ownership and control of the server, it remains unclear what would entitle Moser and RCM Digesters to the server absent that agreement.

The District Court rejected the Biothane parties' arguments that the litigation hold letter or the Federal Rules of Civil Procedure authorized their access, finding the Biothane parties did not act in order to preserve documents for litigation. In doing so, the court appeared to have made a credibility judgment on the deposition testimony of Jay Murphy that he ordered Biothane's employees to access the server and copy files in order to preserve documents for litigation. "Although a 'scintilla of evidence' supporting the non-movant's case is not sufficient to defeat a motion for summary judgment, . . . a district court should not weigh the evidence and determine the truth of the matter itself . .

. ." *Country Floors, Inc. v. Partnership Composed of Gepner & Ford*, 930 F.2d 1056, 1061-62 (3d Cir. 1991) (citing *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 252 (1986)).

Given the awkward procedural posture here, where substantive claims arose from discovery misconduct, we can easily understand how a court might apply an earlier credibility finding in ruling on a summary judgment motion. In addressing sanctionable discovery conduct, district courts can find facts and make credibility determinations. *See Bowers v. NCAA*, 475 F.3d 524, 538 (3d Cir. 2007) ("The decision to impose sanctions for discovery violations and any determination as to what sanctions are appropriate are matters generally entrusted to the discretion of the district court." (citation omitted)). It may be different, however, if a credibility determination is made addressing a motion for summary judgment, even if the same conduct serves as the basis for both motions. *See Doeblers*, 442 F.3d at 820. When, as here, substantive claims arise from sanctionable discovery conduct, the trial court is put in the discordant position of finding facts for one order while stating in a parallel order that the same factual issues are in genuine dispute.

Here, the Magistrate Judge had already found the Biothane parties proffered explanation was not credible, when he found access to the server was done for business, not litigation, purposes. It appears the able District Court here incorporated this finding. But owing to a different trial stage when addressing a summary judgment motion, we believe incorporation of the finding was in error.

Faced with concurrent claims of sanctions for discovery abuse and for injunctive

relief because of anti-hacking violations arising from the same conduct,[12] trial courts may encounter special problems. Injunctive relief may be proper before final judgment, but it can create management difficulties. Some commentators have noted that suits under anti-hacking laws have gone beyond the intended scope of such laws and are increasingly being used as a tactical tool to gain business or litigation advantages. *See* Andrew B. Serwin, *Poised on the Precipice: A Critical Examination of Privacy Litigation*, 25 Santa Clara Computer & High Tech. L.J. 883, 887 (2009) ("The [Federal Computer Fraud and Abuse Act] was an anti-hacking law that has grown well beyond its original role. Now, it can serve as the basis of litigation by creative plaintiffs' class action attorneys, as well as companies attempting to protect their trade secrets."); Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publically Accessible Internet Websites*, 63 Md. L. Rev. 320, 324 (2004) (noting that although some "actions may fall within the literal language of the CFAA, such cases were never intended to be covered by the statute").

Normally discovery misconduct is addressed through sanctions under the Federal Rules of Civil Procedure. Depending on the facts, early resolution of substantive anti-

[12] Other courts and commentators have addressed such a situation. A litigant who, in seeking emails of the opposing parties, served the opposing parties' internet service provider with an overbroad subpoena was both sanctioned and found liable under anti-hacking laws for accessing the emails via the overbroad subpoena. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004); *see also* Adam I. Cohen & David J. Lender, Electronic Discovery: Law & Practice § 11.04 (Supp. 2010) (noting the need to understand "the limitations that [anti-hacking] statutes may place on electronic discovery").

hacking claims arising from discovery misconduct may be necessary, but it may also impact the course of the litigation. Litigants may seek to use that tool to gain litigation advantage. Also, resolution of anti-hacking claims for misconduct during discovery short-circuits the normal course of litigation and permits litigants to obtain interlocutory review. *See* 28 U.S.C. § 1292(a)(1) (granting jurisdiction over "appeals from" orders "granting, continuing, modifying, refusing or dissolving injunctions, or refusing to dissolve or modify injunctions").[13] If the matter can be addressed in a discovery order, it can be reviewed along with the merits after final judgment, making for more efficient adjudication of claims.

III.

For the foregoing reasons we will vacate the order of the District Court partially granting summary judgment against the Biothane parties and remand for further proceedings consistent with this opinion.

[13] Interlocutory review delays the proceedings in the trial court and also burdens litigants and the courts with additional work and costs. *See Cleveland Hair Clinic, Inc. v. Puig*, 104 F.3d 123, 125-26 (7th Cir. 1997) (stating that, in an appeal in which sanctionable conduct overlapped with the merits of the action, "[m]ultiplication of appeals would delay final adjudication and increase the expense of getting there, without producing material benefits").