PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 04-4254

P.C. YONKERS, INC; PARTY CITY CLIFTON, INC.;
PARTY CITY OF HAMILTON SQUARE, INC.;
PARTY CITY OF LAWRENCEVILLE, INC.;
PARTY CITY NORTH BERGEN, INC.;
P.C. VOORHEES, INC.;
EAST HARRISBURG, P.C., INC.;
LANCASTER P.C., INC.;
MONTGOMERYVILLE P.C., INC.;
PARTY CITY OF COTTMAN AVENUE, INC.;
PARTY CITY OF HARRISBURG, INC.;
PARTY CITY OF LEHIGH VALLEY, INC.;
PARTY CITY OF READING, INC.;
CITY OF SPRINGFIELD, INC.;
PARTY CITY OF NEW YORK, INC.;
SCRANTON PARTY CITY LLC;
STROUDSBURG P.C. INC.;
WILKESBARRE PARTY CITY LLC;
PARTY CITY MANAGEMENT, CO., INC.,
Appellants

v.

CELEBRATIONS THE PARTY AND
SEASONAL SUPERSTORE, LLC;
ANDREW BAILEN; ANDREW HACK

Appeal from the United States District Court
for the District of New Jersey
(D.C. Civil No. 04-cv-04554)
District Judge: Honorable Joseph A. Greenaway, Jr.

Argued June 28, 2005

Before: ROTH, RENDELL, and BARRY, Circuit Judges.

(Filed: November 7, 2005)

Keith L. Leiby, Jr.
Shackleton & Hazeltine
159 Millburn Avenue
Millburn, NJ 07041

Michael Einbinder [ARGUED]
Einbinder & Dunn
104 West 40th Street
New York, NY 10018
Counsel for Appellants

Karol C. Walker [ARGUED]
St. John & Wayne
Two Penn Plaza East
Newark, NJ 07105
Counsel for Appellees
Celebrations the Party and
Seasonal Superstore, LLC;
Andrew Bailen

Peter L. MacIsaac [ARGUED]
Chasan, Leyner & Lamparello
300 Harmon Meadow Boulevard
Secaucus, NJ 07094
Counsel for Appellee
Andrew Hack

OPINION OF THE COURT

RENDELL, Circuit Judge.

Plaintiffs P.C. of Yonkers, Inc., and eighteen related "Party City" affiliates (the "PC plaintiffs") appeal the District Court's order denying injunctive relief sought pursuant to the provisions of the federal Computer Fraud and Abuse Act ("CFAA"), and under New Jersey state law. We will affirm because we agree with the District Court's analysis regarding the lack of evidentiary basis for the injunction, but we will take this opportunity to clarify the scope of relief available under CFAA's provisions.

The seventeen Party City retail store plaintiffs are all franchisees of Party City Corporation ("PCC"). Each operates a retail store selling discount party goods and related products (the "PC Stores"). Plaintiff Party City Management Co., Inc. ("PC Management"), manages the operations of the franchised locations. Defendant Andrew Hack ("Hack") worked for PCC in various positions from March 1991 until his termination in August 2003. He continued to act as a consultant to PC Management from September 11, 2003 to November 25, 2003. Defendant Andrew Bailen ("Bailen"), also a longtime PCC employee, served as the company's executive vice president for merchandise and marketing from August 2000 until he left its employ on July 14, 2003.

In 2004, Bailen and Hack formed Celebrations! The Party and Seasonal Superstore, L.L.C. ("Celebrations"), also a defendant in this case, and opened two of its own retail party goods stores in the vicinity of two existing PC Stores, one in Greenburgh, New York, and a second in Clifton, New Jersey, in late July and August of 2004, respectively. The PC plaintiffs averred that the Celebrations stores opened "just in time to compete with plaintiff PC stores during the biggest selling season – the weeks leading up to Halloween," and that "sales during this time of year are critical to a successful business year." (Compl. ¶ 36.)

The PC plaintiffs' primary claim under CFAA was that defendant Hack, "without authorization and on behalf of defendant Celebrations and defendant Bailen," accessed PCC's Tomax computer system from his home 125 times over seven days during October and November of 2003. Eight of the

alleged incursions occurred after Hack ceased working as a consultant to PC Management.[1] Additionally, plaintiffs claim that unauthorized access purportedly was gained again in December 2003 and a final time in April 2004, when Hack was no longer associated with any of the PC plaintiffs.

The access in December 2003 lasted a total of 19.4 minutes. Hack testified that he had a home office during his years with PCC and had been authorized to use his computer from home; as proof, he offered e-mails demonstrating that he did so. He could not recall making this particular access but stated that he imagined it would have been for PC Management business as he never accessed the Tomax system for anything but PC Management related work. The PC plaintiffs contested Hack's asserted authorization in their submissions. The April access was for a total of 5 minutes and 49 seconds, and Hack testified that it appears to have been an automatic redial of the last call he had made to the PC Lancaster store in December. There is a paucity of information as to precisely what could have been obtained from the system in these incursions, although the PC plaintiffs' computer consultant, Joseph Savin, stated that "reports" could be ordered in a matter of seconds and then "later, with a few keystrokes," downloaded and sent to a remote location. (Savini Certification ¶ 6, Oct. 8, 2004.)

The PC plaintiffs averred that the defendants used the information obtained from this access to decide where to locate

---

[1]It is undisputed that Hack ceased consulting for PC Management on November 25, 2003.

their stores, where to focus marketing efforts and budgets, and to obtain valuable information as to sales during the Halloween season. They urge that by using this valuable information, defendants purportedly obtained an unfair competitive advantage. The PC plaintiffs specifically averred that defendants' unauthorized access resulted in damage or loss to the PC plaintiffs of not less than $5,000 within the meaning of CFAA, 18 U.S.C. § 1030.

The PC plaintiffs sought an injunction prohibiting Celebrations from operating the Celebrations stores and from using the PC plaintiffs' trade secrets and confidential and proprietary information, and ordering the return of such information. They also averred that defendants' conduct violated New Jersey statutory and common law, entitling the PC plaintiffs to damages.

After limited discovery, the District Court heard oral argument on the motion and expressed doubt that 18 U.S.C. § 1030, which is primarily a criminal statute, provided for any civil relief. However, the District Court reasoned that even if the statute were read to provide a civil remedy, the PC plaintiffs had failed to frame their claim as a claim under subsection (a)(5) of § 1030, and thus were not entitled to injunctive relief under CFAA. Further, the District Court held that, even if a claim could properly be brought under subsection (a)(4) of § 1030, the PC plaintiffs had failed to demonstrate a likelihood of success on the merits of such a claim, because they had not shown what, "if anything, was actually taken from the Tomax system [by defendants], nor for that matter, confirm with certainty that the incursions were inappropriate or outside the scope of a

legitimate work purpose."[2] (Trans. of Op. at 34.)

The Court also ruled that the PC plaintiffs had not demonstrated that they would succeed under the related New Jersey statute prohibiting certain computer incursions, or on the merits of their common law trade secret misappropriation claim. This latter finding was based on the PC plaintiffs' failure to prove that the information in the Tomax system was indeed entitled to protection as a "trade secret" and also because monetary damages would compensate for any injury, thus making injunctive relief inappropriate.

The District Court had jurisdiction over this matter pursuant to 18 U.S.C. § 1030 and 28 U.S.C. §§ 1331 and 1367. Our jurisdiction over this appeal from an interlocutory order arises under 28 U.S.C. § 1292(a)(1).

This Court has held that a district court may permissibly grant the "extraordinary remedy" of a preliminary injunction only if "(1) the plaintiff is likely to succeed on the merits; (2) denial will result in irreparable harm to the plaintiff; (3) granting the injunction will not result in irreparable harm to the defendant; and (4) granting the injunction is in the public interest." *Nutrasweet Co. v. Vit-Mar Enterprises*, 176 F.3d 151, 153 (3d Cir. 1999) (quoting *Maldonado v. Houstoun*, 157 F.3d 179, 184 (3d Cir. 1998)). The burden lies with the plaintiff to establish every element in its favor, or the grant of a preliminary

---

[2]We do not distinguish among the defendants in terms of the conduct complained of, as it is not necessary to our ruling.

injunction is inappropriate. *See id.*

We review the denial of a preliminary injunction for "an abuse of discretion, an error of law, or a clear mistake in the consideration of proof." *Kos Pharms., Inc. v. Andrx Corp.*, 369 F.3d 700, 708 (3d Cir. 2004) (quotation omitted). "Any determination that is a prerequisite to the issuance of an injunction . . . is reviewed according to the standard applicable to that particular determination." *Id.* Therefore, we exercise plenary review over the district court's conclusions of law and its application of law to the facts, but review its findings of fact for clear error. *Duraco Prods., Inc. v. Joy Plastic Enters., Ltd.*, 40 F.3d 1431, 1438 (3d Cir. 1994).

DISCUSSION

(1) Denial of Injunctive Relief.

We will not disturb the District Court's ruling that if § 1030(g) is interpreted as providing a civil remedy, and injunctions in aid thereof, the PC plaintiffs failed to prove that they were likely to succeed on the merits of their claim because they failed to demonstrate any conduct on the part of defendants other than the alleged access (which may or may not have been authorized). As the District Court correctly found, there is absolutely no evidence as to what, if any, information was actually viewed, let alone taken. Lacking such a showing, the elements of the causes of action brought by the PC plaintiffs cannot succeed.

The federal and state law causes of action asserted

by the PC plaintiffs have several elements. It is undisputed that the conduct complained of falls under subsection (a)(4) of § 1030. A claim under CFAA § 1030(a)(4) has four elements: (1) defendant has accessed a "protected computer;" (2) has done so without authorization or by exceeding such authorization as was granted; (3) has done so "knowingly" and with "intent to defraud"; and (4) as a result has "further[ed] the intended fraud and obtain[ed] anything of value." 18 U.S.C.A. § 1030(a)(4); *see also Pacific Aerospace & Elecs., Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1195 (E.D. Wash. 2003).

New Jersey state law provides that any person "damaged in business or property" as a result of "[t]he 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," may recover damages. N.J. Stat. Ann. § 2A:38A-3(a). Lastly, under New Jersey law, to establish a claim for misappropriation of a trade secret, a plaintiff must show, *inter alia*, the existence of a trade secret and that it was "acquired by the competitor with knowledge of the breach of confidence." *Rohm & Haas Co. v. Adco Chem. Co.*, 689 F.2d 424, 429-30 (3d Cir. 1982). Whether or not the data at issue here was a trade secret, there has been no showing that anything was "acquired" by defendants.

It is clear that PC plaintiffs do not know, have not shown, and cannot show, what information, if any, was taken. Mr. Nasuti, president of PC Management, stated repeatedly in his deposition that plaintiffs do not know what, if anything, was

actually taken, much less information that could be deemed to be a trade secret, and this is uncontroverted. In fact, no proof of conduct other than access has been shown, thus dooming both of the New Jersey state law claims, which require proof of some activity vis-a-vis the information other than simply gaining access to it.[3]

Under CFAA, too, more is required. The third and fourth elements we cite above – (3) knowingly and with intent to defraud, and (4) as a result . . . furthered the intended fraudulent conduct and obtained anything of value – pose hurdles that PC plaintiffs have not demonstrated they can overcome.

The only evidence that might arguably support an inference as to these elements consists of a one-line e-mail sent in December 2003 by Hack to Savin, seeking SKU numbers "confidentially." Access occurred from Hack's home computer later that month. While this raises some level of suspicion, without more we cannot infer anything of probative value. It is too slim a reed upon which to rely as proof of the necessary elements under CFAA.

---

[3] We need not address separately the District Court's ruling regarding trade secrets or the availability of monetary relief, as we affirm all aspects of the District Court's ruling based on the general ground that absent proof of something more than mere access, whether or not the information in the system was secret, there can be no likelihood of success on any of the state law claims asserted.

The PC plaintiffs urge that we draw inferences of intent and the obtaining of valuable information from the mere fact that unauthorized access has been shown, and ask defendants to rebut these inferences by demonstrating the innocence of their purpose or actions. However, the elements of the claims asserted are part of a *plaintiff's* burden. That information was taken does not flow logically from mere access. Access could be accidental, and, even if access were purposeful and unauthorized, information could be viewed but not used or taken. Furthermore, without a showing of some taking, or use, of information, it is difficult to prove intent to defraud, and indeed, the PC plaintiffs have not shown that they can do so.

Here, the PC plaintiffs needed something more. Perhaps they could have produced evidence of identical merchandise code numbers (known as SKUs) in the Celebrations stores, or of vendors contacted by Hack or Bailen in temporal proximity to the unauthorized access. Or, perhaps, they could have adduced evidence tending to show that neither Hack nor Bailen could independently have started and stocked the Celebrations stores. But, absent any such evidence, the logical inference is not that there was access and use of information that harmed them, but, to the contrary, that in opening and stocking their stores, defendants Bailen and Hack were employing their expertise gained through years of experience in the retail party goods business, unaided by any information obtained through access to the PC plaintiffs' computer system.

Bailen had been the number two executive for PCC before leaving in 2003, and had had the direct

responsibility for all of its buying, marketing, visual merchandising planning, and allocation of supply chain efforts for over 500 stores nationwide. The record contains the numerous e-mails sent by Hack over the relevant time period pertaining to his plans and the steps he was taking with Bailen to start Celebrations, none of which contains any reference to any outside information. Nor do PC plaintiffs point to any conduct by Hack or Bailen that might imply use of any type of information gained from the Tomax system.

We have only the unauthorized access in December 2003 and then again in April 2004, and PC plaintiffs' failure to complain prior to their bringing an injunction motion in September 2004, when the Halloween season was imminent. This does not satisfy the proof necessary for injunctive relief in aid of the claims at issue.

Accordingly, we agree with the District Court that the PC plaintiffs' proffer was not sufficient and that due to the speculative nature of their proof, they failed to demonstrate that they could succeed on the merits of any of their claims so as to warrant injunctive relief.

(2) CFAA

The District Court struggled with the meaning of, and relationships among, various provisions of CFAA. It is, as the District Court noted, a criminal statute, criminalizing and penalizing unauthorized access to computers, and, as noted by the Court in *Pacific Aerospace*, the majority of CFAA cases still involve "classic" hacking activities. 295 F. Supp. 2d at 1196.

However, the scope of its reach has been expanded over the last two decades. "Employers ... are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system." *Id; see also Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1124 & n.3 (W.D. Wash. 2000) (explicitly recognizing that Congress' 1994 amendment to the CFAA added a private cause of action under § 1030(g)).

As currently in force, 18 U.S.C. § 1030 lists seven different types of conduct punishable by fines or imprisonment. These are set forth in subsection 1030(c). The prohibited conduct ranges from trafficking in passwords to knowing and unauthorized access to government computers. Subsection 1030(d) grants authority to various agencies of the federal government to investigate offenses. Subsection 1030(e) contains definitions, while subsection (f) provides that the powers under the federal law are not exclusive of state powers. Subsection (g) – containing the purported civil remedy at issue here – provides:

> (g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section

> may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

18 U.S.C. § 1030(g).

The District Court focused on the criminal provisions and found it difficult to infer a civil application within the statutory framework and concluded that it could not do so, although the Court did acknowledge that several other courts had determined to the contrary. However, we conclude that not only the relevant case law, but also the plain language of the statute, militate in favor of the availability of a civil remedy, and specifically, the type of injunctive relief sought by the PC plaintiffs.

Numerous courts have recognized that a civil

cause of action is apparent from the text of § 1030(g). Although we acknowledge the criminal thrust of the section in general, as it is found in Title 18, there is ample authority for permitting civil actions to proceed based on violations of the section pursuant to the language of § 1030(g). *See*, *e.g.*, *Theofel v. Farey-Jones*, 359 F.3d 1066, 1078 (9th Cir. 2003) ("The civil remedy extends to '*[a]ny person* who suffers damage or loss by reason of a violation of this section.'") (emphasis in original); *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 526 (S.D.N.Y. 2004) (stating that § 1030(g) affords civil action for any violation of CFAA). Accordingly, we conclude that civil relief is available under § 1030(g).

Defendants make a novel argument, however, in an attempt to undercut the availability of relief here. They posit that the third sentence of subsection (g) – which limits recovery to only economic damages for a violation solely involving conduct described in subsection (a)(5)(B)(i) – also operates to exclude injunctive relief for claims involving such conduct. That reading is unwarranted. We read that sentence to mean, instead, that if one who is harmed does seek compensatory damages based on such conduct, which are available by virtue of the general statement contained in the first sentence, then *those* damages will be so limited. That is, compensatory damages for such conduct will be awarded only for economic harm. Nothing in the third sentence, however, countermands or limits the type of injunctive relief specifically authorized in the first sentence of (g). In fact, two courts have held that the third sentence does not even limit all compensatory damage claims but only those based on the specific subsection of § 1030 referred to in the third sentence. *See In re Intuit Privacy Litig.*,

138 F. Supp. 2d 1272, 1281 (C.D. Cal. 2001); *In re Doubleclick Privacy Litig.*, 154 F. Supp. 2d 497, 519-526 (S.D.N.Y. 2001).[4] Accordingly, claims for other types of compensatory damages – for conduct other than violations of (a)(5)(B)(i) – are clearly allowed, as are claims for any and all types of injunctive relief.

The only remaining issue pertains to an aspect of section 1030(g) that was also of concern to the District Court. That is, does the reference in section 1030(g) to subsection (a)(5)(B) preclude relief for violations that are brought – as PC plaintiffs' is – under subsection (a)(4)? We conclude that it does not, provided that the claim brought under subsection (a)(4) – or any other section for that matter – "involves" one of the five enumerated results in § 1030(a)(5)(B)(i)-(v). For ease of reference, we repeat both section 1030 (a)(4) and (a)(5) in the footnote below.[5]

---

[4]These cases concerned specific language found in a prior version of § 1030(g) – before the October 26, 2001 amendments to the statute. *See* 18 U.S.C. § 1030 (1996) (*amended by* current version at 18 U.S.C. § 1030(g)). The third sentence then referred to violations involving damage as defined in subsection (e)(8)(A), *id.*, whereas the current version references (a)(5)(B)(i), *see* 18 U.S.C. § 1030 (g) (2005).

[5]18 U.S.C. § 1030(a): ... (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of

Here, PC plaintiffs' claim is clearly based on a

---

the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related courts of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security; . . .

violation of (a)(4), but they included in their complaint a specific allegation of loss in excess of $5,000, which satisfies (a)(5)(B)(i). We do not read section 1030(g)'s language that the claim must *involve* one or more of the numbered subsections of subsection (a)(5)(B) as limiting relief to claims that are *entirely based only on* subsection (a)(5), but, rather, as requiring that claims brought under other sections must meet, in addition, one of the five numbered (a)(5)(B) "tests." *See I.M.S.*, 307 F. Supp. 2d at 526. Otherwise, the language would not have referred to one or more of the numbered subsections, but would have said that relief is only available for claims under subsection (a)(5). We must take Congress' use of language as purposeful. *See Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253-54 (1992) (noting that "courts must presume that a legislature says in a statute what it means and means in a statute what it says"). Accordingly, we conclude that the claim asserted by PC plaintiffs fits squarely within the class of claims eligible for injunctive relief, for it involves one of the factors contained in subsection (a)(5)(B), namely, the $5,000 loss provision of (a)(5)(B)(i).

We note that one court seems to have read section 1030(g)'s reference to subsection (a)(5)(B) as limiting relief under section 1030(g) to only subsection (a)(5) claims, but we disagree. *See McLean v. Mortg. One & Fin. Corp.*, 2004 U.S. Dist. LEXIS 7279, *5 (D. Minn. Apr. 9, 2004). The weight of authority is clearly to the contrary. *See Theofel*, 359 F.3d at 1078 ("The conduct must involve one of five factors listed in 18 U.S.C. § 1030(a)(5)(B), which include a loss in excess of $ 5000.")*; Nexans Wires S.A. v. Sark-USA, Inc.*, 319 F. Supp. 2d 468, 472 (S.D.N.Y 2004) (holding that requirement is met where

plaintiff meets the jurisdictional threshold by asserting loss in excess of $5,000 under (a)(5)(B)(i)); *I.M.S.*, 307 F. Supp. 2d at 526 (holding that subsection (g) affords a civil action for any CFAA violation, but "requires an allegation of one of the five enumerated factors in § 1030(a)(5)(B)).

CONCLUSION

We conclude that although the PC plaintiffs' claim for injunctive relief under CFAA is cognizable under the statutory framework and language, and we therefore disagree with the District Court to the extent it opined to the contrary, we will AFFIRM the judgment of the District Court that the PC plaintiffs failed to adduce sufficient proof of a violation under CFAA and were therefore not entitled to injunctive relief under that statute or under applicable New Jersey law.